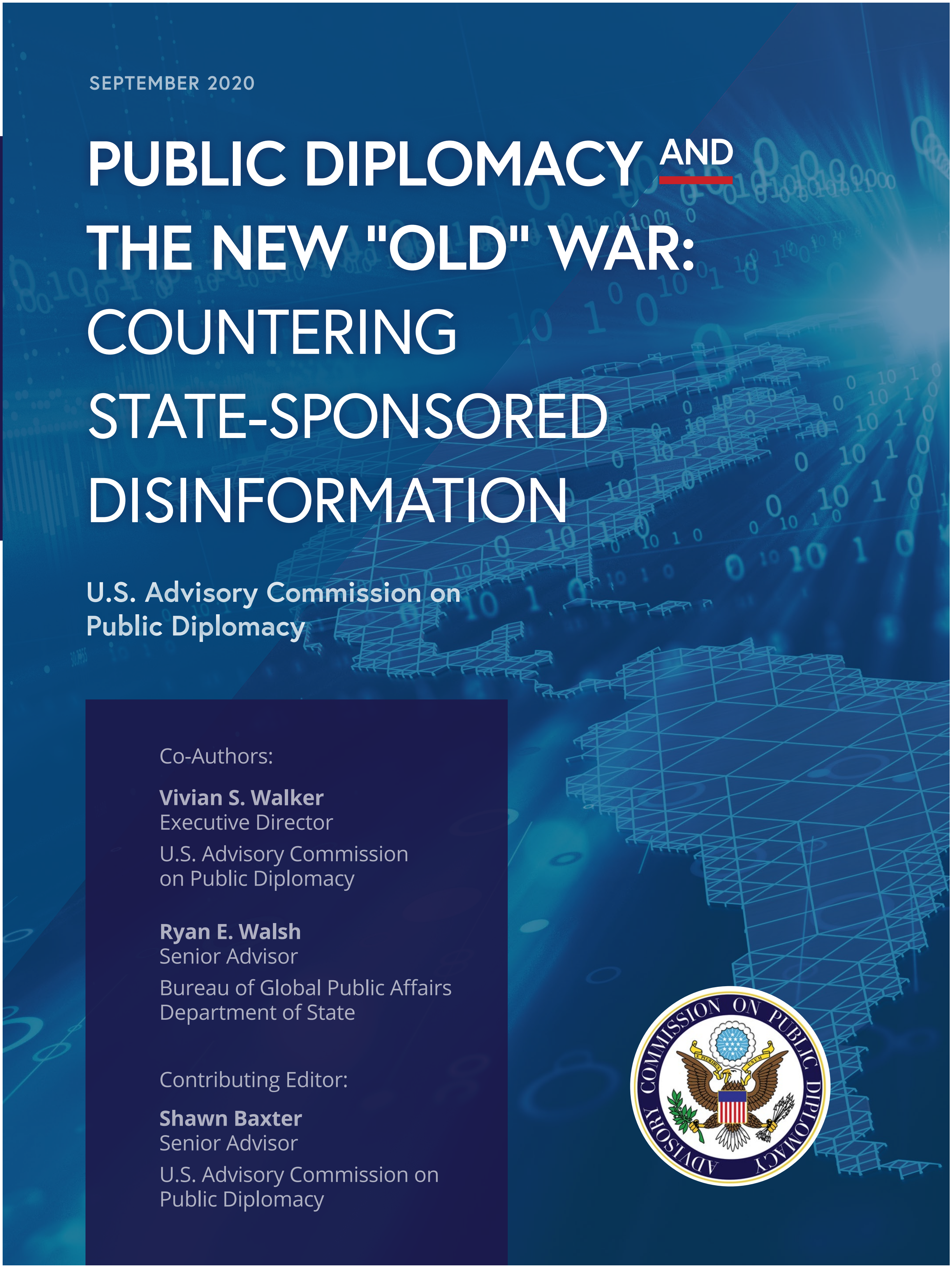


SEPTEMBER 2020

PUBLIC DIPLOMACY AND THE NEW "OLD" WAR: COUNTERING STATE-SPONSORED DISINFORMATION

U.S. Advisory Commission on
Public Diplomacy

Co-Authors:

Vivian S. Walker
Executive Director
U.S. Advisory Commission
on Public Diplomacy

Ryan E. Walsh
Senior Advisor
Bureau of Global Public Affairs
Department of State

Contributing Editor:

Shawn Baxter
Senior Advisor
U.S. Advisory Commission on
Public Diplomacy

TABLE OF CONTENTS

TO THE PRESIDENT, CONGRESS, SECRETARY OF STATE AND THE AMERICAN PEOPLE:

The United States Advisory Commission on Public Diplomacy (ACPD), reauthorized pursuant to Public Law 114-323, hereby submits this special report, *Public Diplomacy and the New "Old" War: Countering State-Sponsored Disinformation*.

The ACPD is a bipartisan panel created by Congress in 1948 to appraise all U.S. government efforts to understand, inform, and influence foreign publics. The Commission makes recommendations to improve the Public Diplomacy (PD) functions vested in U.S. government entities such as the Department of State, the U.S. Agency for Global Media, and other interagency partners.

U.S. government public diplomacy efforts are increasingly challenged by a sophisticated array of technology-enabled, information-based threats. Disinformation, or the manipulation and dissemination of information to adversely influence public perceptions and behaviors, has emerged as a major destabilizing force in the global information space. These sophisticated threats weaken state credibility, perpetuate destabilizing narratives about national identity and values, and, most dangerously, erode public confidence in democratic institutions.

The ACPD's May 2017 special report *Can Public Diplomacy Survive the Internet?* examined aspects of the disinformation threat and the implications for the future of public diplomacy programming. One danger featured in the 2017 report—state-sponsored disinformation—remains a particular concern. In addition to assessing recent Department of State and U.S. Agency for Global Media efforts to counter this growing threat, this report offers a set of recommendations that balance longer-term resilience and capacity building measures with shorter time horizon initiatives such as deterrence and messaging.

We greatly appreciate the skill and dedication of public diplomacy practitioners at home and abroad who serve on the front lines of the geostrategic competition for influence in the global information space.

Respectfully Submitted,

Sim Farar

Sim Farar
Chairman
(California)

William J. Hybl

William J. Hybl
Vice Chairman
(Colorado)

Anne

Anne Wedner
(Illinois)

ACKNOWLEDGEMENTS

This publication benefited enormously from expertise provided by an outstanding group of public diplomacy practitioners, policymakers, researchers, and scholars.

The authors would like to extend special thanks to the following individuals and institutions:

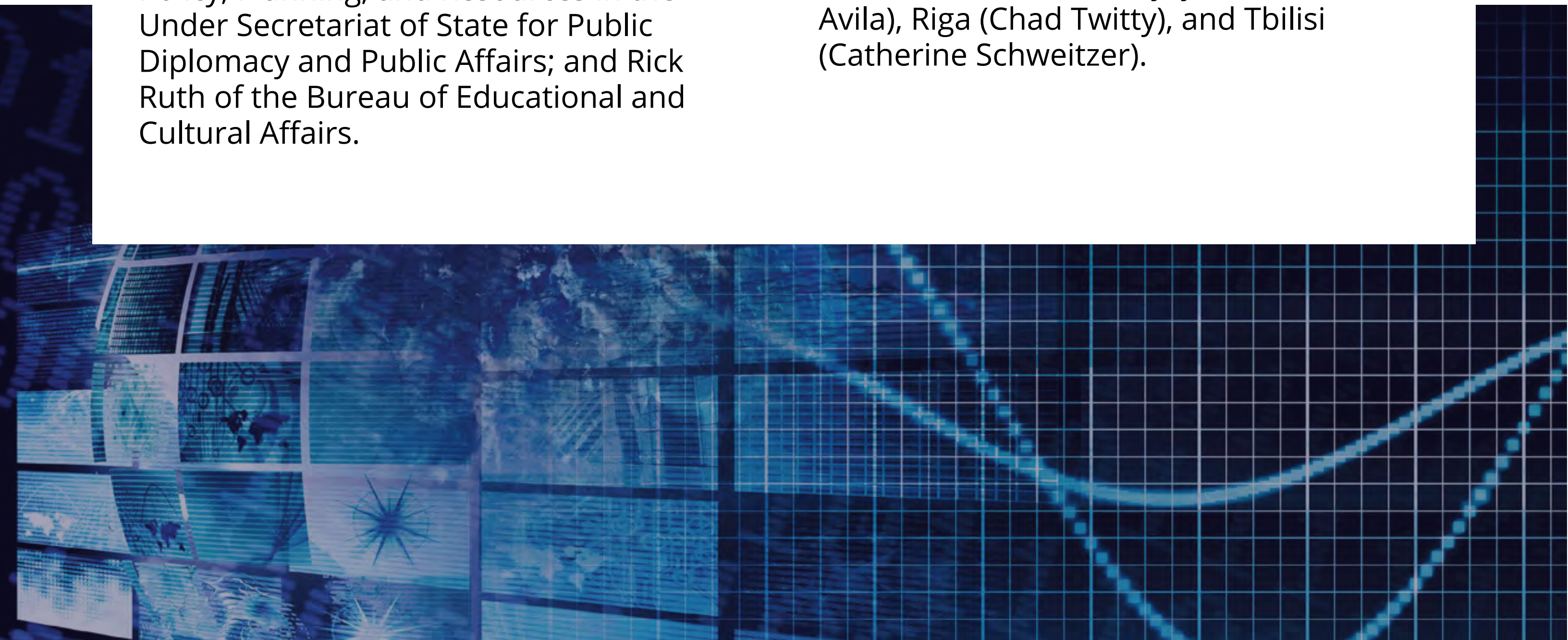
Former acting ACPD Executive Director Ambassador Jeff Daigle; current and former members of the State Department public diplomacy community, including Under Secretaries for Public Diplomacy and Public Affairs Ambassador Bruce Wharton and Richard Stengel; Macon Phillips, former Coordinator of the Bureau of International Information Programs; Daniel Kimmage of the Global Engagement Center; the Bureau of Global Public Affairs, its Research and Analytics team, especially Brittany DiPaolo; Brian Heath and Andy Loomis of the Office of Policy, Planning, and Resources in the Under Secretariat of State for Public Diplomacy and Public Affairs; and Rick Ruth of the Bureau of Educational and Cultural Affairs.

We also extend our thanks to other key elements of the wider public diplomacy community such as:

The U.S. Agency for Global Media, especially Shawn Powers and Olga Stefanou, and external experts including Graham Brookie of the Digital Forensics Research Lab (Atlantic Council); Bret Schafer of the Alliance for Securing Democracy (German Marshall Fund); and Matt Armstrong.

Additionally, we wish to thank the dedicated public diplomacy officers and locally employed staff at:

U.S. embassies in Budapest (Diana Sitt), Helsinki (Bill Couch), Reykjavik (Oscar Avila), Riga (Chad Twitty), and Tbilisi (Catherine Schweitzer).



We would also like to acknowledge the following host country officials and academic and policy experts for their invaluable insights.

Budapest, Hungary: Political Capital—Péter Krekó, Executive Director, and Lóránt Győri, Geopolitical Analyst; Nézőpont Institute's Media Observer Center—Levente Bánk Boros; Mérték Media Monitor—Gábor Polyák; Center for Media, Data and Society at the Central European University—Marius Dragomir, Director, and Éva Bognár, Senior Program Officer; National Public Service University representatives; and the *Heti Világgazdaság* (HVG) editorial team.

Riga, Latvia: Ministry of Culture—Zane Vāgnere, Deputy State Secretary, Andris Mellakauls, Head of Information Space Integration Division, and Klinta Locmele, Media Policy Department; Viktors Makarovs, Ministry of Foreign Affairs; and Janis Sarts, Director, NATO Stratcom Centre of Excellence.

Helsinki, Finland: Jussi Toivanen, Chief Communications Specialist, Government Communications; and staff members at the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE).

Reykjavik, Iceland: Silja Bara Omarsdottir, University of Iceland Institute for International Affairs; Maria Mjoll Jonsdottir, Ministry for Foreign Affairs; and Elfa Yr Gylfadottir, Director, Media Commission.

Tbilisi, Georgia: Ekaterine Metreveli, Director, Georgian Foundation of Strategic and International Studies; Tamar Kintsurashvili, Executive Director, Media Development Foundation; Maia Mikashavidze, Georgian Institute for Public Affairs; Ramaz Aptsiauri, United Nations Association of Georgia; and Giorgi Goguadz, Director, Georgian Center for Strategy and Development.

Public Diplomacy and the New "Old" War: Countering State-Sponsored Disinformation

EXECUTIVE SUMMARY

United States government Public Diplomacy (PD) efforts are increasingly challenged by a sophisticated array of technology-enabled, information-based threats. Disinformation, or the manipulation and dissemination of information to adversely influence public perceptions and behaviors, has emerged as a major destabilizing force in the global information space. These sophisticated threats weaken state credibility, perpetuate destabilizing narratives about national identity and values, and, most dangerously, erode public confidence in democratic institutions.

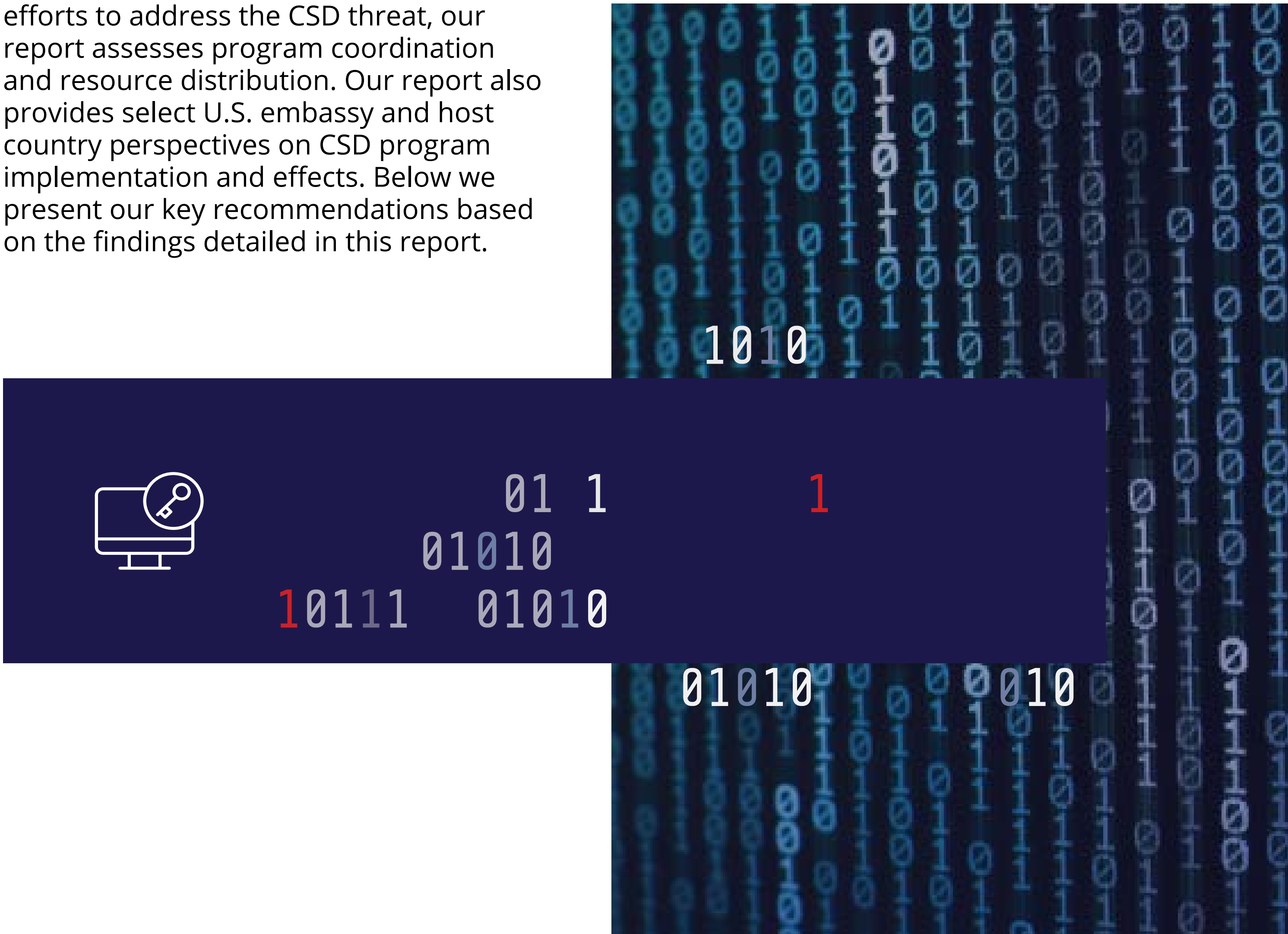
The U.S. Advisory Commission on Public Diplomacy's (ACPD) May 2017 special report *Can Public Diplomacy Survive the Internet?* examined aspects of the disinformation threat and the implications for the future of public diplomacy programming. One danger featured in the report—state-sponsored disinformation—remains a particular concern. This report assesses recent Department of State and U.S. Agency for Global Media (USAGM) efforts to counter this growing threat.

Beginning in 2016, the U.S. government (USG) made a concerted effort to adjust its resources in order to counter the resurgent threat of disinformation. At first, the response was uncoordinated, with many actors responding independently based on their policy focus. However, with the passage of the 2017 National Defense Authorization Act (NDAA), which created the Global Engagement Center (GEC), a coordinated effort to counter disinformation effects began to take shape. In addition to the GEC's mandate to support and coordinate USG counter malign influence efforts, the Department of State acquired new technical capabilities for the monitoring of disinformation and dissemination of targeted messaging.

Legacy State Department public diplomacy bureaus, such as Educational and Cultural Affairs (ECA), acquired new vehicles for funding and programming against state-sponsored disinformation. Meanwhile, the Department of State merged the Bureau of International Information Programs (IIP) and the Bureau of Public Affairs (PA), creating the Bureau of Global Public Affairs (GPA) to actively increase engagement in the global online conversation. Finally, as part of its rebranding effort, the U.S. Agency for Global Media launched an ambitious series of counter disinformation program initiatives, incorporating new technologies while building on existing infrastructure.

It is clear that there already is a considerable amount of interagency activity focused on countering state-sponsored disinformation (CSD). However, as new workflows and authorities are established to support existing resources, actors (offices, bureaus or agencies, field posts, etc.) with equities in countering the disinformation threat are increasingly siloed, reporting on their activities through narrow bureaucratic channels. This atomization of effort not only mitigates against a coordinated response but limits a broader understanding of how USG PD treats this issue overall, a deficit this special report intends to address. In addition to offering a unique diagnostic assessment of recent PD efforts to address the CSD threat, our report assesses program coordination and resource distribution. Our report also provides select U.S. embassy and host country perspectives on CSD program implementation and effects. Below we present our key recommendations based on the findings detailed in this report.

Actors...with equities in countering the disinformation threat are increasingly siloed, reporting on their activities through narrow bureaucratic channels.



RECOMMENDATIONS

1 | DEFINE.

Define the CSD challenge with a Department-wide lexicon of disinformation.

A simple Google search turns up hundreds of ways to describe aspects of malign influence operations: misinformation, disinformation, propaganda, information operations, and psychological operations, to name just a few. This lack of consensus on basic terms creates vulnerabilities for internal bureau, agency, or institutional efforts, as well as significant challenges to interagency or joint operations. Without agreed-upon definitions, it is hard to come to a shared understanding of the threat, to define a set of common strategic objectives, or to concur on desired outcomes. It is also difficult to assess impact and define success—or failure—when a number of distinct and even competing definitions are in play. Moreover, competing definitions that fall along internal bureau and division lines discourage the creation of Department-wide CSD initiatives. Reliable deterrence measures begin with the establishment of a lexicon of disinformation—a generally agreed-upon set of related terms and definitions.

2 | INVEST.

Invest more in digital capabilities, but not at the expense of long-term person-to-person initiatives.

Everyone the ACPD interviewed concurred that the U.S. government has not yet marshalled enough resources to combat this already complex and evolving threat. More investment is required in the identification and development of digital tools. Because these new tools produce an intensive competition for resources to develop and implement them, we must also be able to identify which of them are the most cost effective and produce the greatest impact relative to the investment in money and personnel. At the same time, now is not the moment to abandon the proverbial last three feet. It is absolutely necessary to step up existing educational exchange and training programs that focus on building resilience to disinformation effects through media literacy, capacity building, and content support for local independent media outlets and successor generation outreach initiatives.

3 | COMPETE.

Compete in the information space by restructuring overseas PD sections with teams dedicated to modern digital communications.

The private sector learned long ago that online brand and image management was not only a critical component of overall marketing activities, but also that it requires a full-time staff of specialized team members. PD sections at USG posts should be no different in that regard. However, public diplomacy officers and their staffs are tasked with managing a full suite of PD activities in addition to overseeing digital programming and outreach requirements. Further, sensitivities around host governments and/or shared adversaries complicate attempts at active messaging in the digital media space. The ongoing PD Staffing Initiative being led by the Under Secretary for PD's Office of Policy, Planning, and Resources (R/PPR), part of a larger PD modernization effort that aims to update many of the tools and structures on which PD teams rely in the field, is a step in the right direction, but the pace should be stepped up to better face these digital threats. Front-line PD practitioners must have the capacity to keep up with constantly evolving malign influence operations.

4 | SPECIALIZE.

Create a job series for mid-career CSD specialists.

We need professional expertise to support effective engagement in the digital space, particularly at the field level. As one interviewee told us candidly, "A lot of people understand what the problem is, but not a lot of people know what to do about it. We need a cadre of specialists." We recommend the recruitment of mid-career PD FSOs with expertise unlikely to be acquired through the existing avenues of government recruitment. We also suggest the formation of a forward-deployed information specialist intake program. Given the rapid pace of change, the talent pool should be frequently refreshed.

5 | EXPERIMENT.

Develop mechanisms to rapidly redirect funding to seed programs and allow them to scale or fail—*fast*.

A culture of risk aversion must be overcome to make meaningful improvements. Many PD programs, once established, exist for many years after they are developed. Given that programs conceived today are maintained through multiple assignment-driven personnel shifts, the programming is likely to fall behind the pace of technological change. Yet, practitioners in the digital space improve mainly by iterative programming; they learn what can be achieved through rapid implementation of the best available resources and information. Funding for programming should be merit-based and independently verified to ensure it is modern and effective.

6 | EVALUATE.

Evaluate, monitor, and assess the impact of CSD programs.

This ACPD report is the first attempt at a broad examination of USG PD CSD programming. However, more needs to be done to identify gaps in programming in order to adjust resources to meet emergent needs – particularly in the rapidly evolving digital space. With respect to internal reviews, R/PPR should monitor all CSD programs by a budgetary funding code in order to assure accurate tracking of expenditures. Meanwhile, to monitor breadth and efficiency of CSD program coverage, GEC should take the lead in identifying strategic programming gaps in priority regions.

Additionally, we recommend an external strategic review of CSD programming. In the last decade the number of State Department initiatives to counter state-sponsored disinformation and malign influence strategies has increased exponentially. The proliferation of these programs risks the imposition of undue administrative burdens on already overstretched Public Affairs Sections (PAS) in the field. It also risks duplication of effort and inefficient resource distribution. An external historical overview of CSD program lessons learned and best practices would not only serve to minimize program inefficiencies but could also establish a baseline for future efforts to measure disinformation impact and effects.

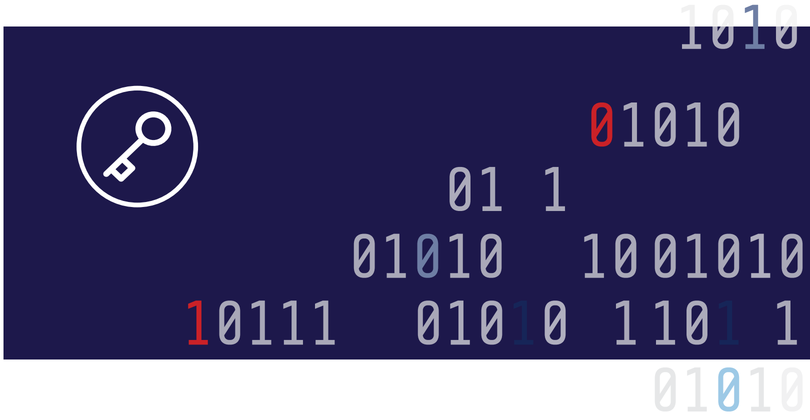
STRUCTURE, METHODOLOGY AND KEY TERMS

Part I of this report represents the culmination of a year of research (2019-2020) on one of the leading foreign policy challenges of our time: how the U.S. government (USG) currently approaches the public diplomacy aspect of countering state-sponsored disinformation.[1] To define the parameters of the problem, the ACPD conducted a number of interviews with key stakeholders including, but not limited to, those currently responsible for leading and/or implementing CSD initiatives, current and former officials, relevant subject matter experts, authors, and academics—at home and abroad. We also performed an independent literature review of the most influential academic studies on the subject, as identified by practitioners and experts themselves.

While this report draws from thought leaders inside and outside government, this has not been solely an academic exercise; the bulk of the input was collected from practitioners themselves, in Washington and the field, as well as from implementers and partners of the wider USG public diplomacy community. Instead of limiting the discussion by preemptively defining the term "disinformation," the data collection process required various actors and implementers to outline what they considered an activity principally designed to achieve CSD goals.

Part II of this report offers a quantitative assessment of CSD programming based on several original data sets. We examined unclassified cable traffic beginning in 2009 to gauge for shifts in PD priorities; we analyzed Integrated Country Strategies, Joint Regional Strategies, and Functional Bureau Strategies for mentions of counter-disinformation; we consulted a database that tracks PD activities called the Mission Activity Tracker for background; and, perhaps most importantly, the ACPD conducted a joint data call with the GEC in which all U.S. missions were requested to report on two years of CSD activities. Other inputs originated from data directly shared with us by the relevant teams.

Part III of this report, structured as a series of mini-case studies, examines field-focused efforts to counter Russian Federation-sponsored disinformation strategies in Europe. Beginning with an overview of current political, social, and economic vulnerabilities to disinformation, the report then addresses country-specific national and institutional experiences of and responses to disinformation effects. These insights are based on in-depth conversations held with U.S. embassy officers administering local public



diplomacy and civil society development programs as well as host country government, NGO, academic, and media representatives with a stake in the effort to mitigate the destabilizing potential of malign influence strategies. The report also provides brief synopses of CSD operations in Public Affairs Sections at U.S. embassies in Iceland, Finland, Latvia, Hungary, and Georgia.

There are several procedural and definitional issues that should be noted prior to any discussion of the findings outlined in this report. First, this report only covers those aspects of CSD programming which fall under the purview of public diplomacy. For the purposes of this report, public diplomacy is defined as official State Department efforts to inform and influence foreign audiences to promote the U.S. national interest and advance key foreign policy goals. This is an important distinction, as nothing in this report will include other aspects of a non-PD nature, unclassified or otherwise.

Second, the term “disinformation” can be used rather freely as a catch-all. However, professionals in this space are quick to acknowledge that in a practical sense, “disinformation” as we know it is not a distinct threat area. Rather it is actually a subset of a larger range of adversarial activities designed to disrupt and weaken opponents, which are commonly known as “malign influence operations.” These operations usually can include other activities such as dark financing, which have little to do with public diplomacy.

As such, any findings in this report should be understood as *intentionally* limited to:

- ***Public diplomacy.*** The wider scope of USG capabilities and tools in countering malign influence activities, or their role in hybrid warfare, are not included.
- ***Foreign activities.*** While discussions of disinformation often get conflated with domestic issues, public diplomacy as a discipline, the ACPD as a federal commission, and this report exclusively focus on activities that take place outside of the United States.
- ***State-sponsored.*** This paper focuses on state-sponsored disinformation threats rather than individuals or non-state groups acting, knowingly or not, to spread false or misleading information.

Given the scope and fast-changing nature of the issue, this report does not attempt to cover the full range of USG programs and activities to counter state-sponsored disinformation, such as those carried out by the U.S. Agency for International Development or the National Endowment for Democracy. Instead, it offers a baseline representation of key initiatives in order to set the stage for a conversation about the way forward. To frame this conversation, this report provides indicators to facilitate program assessment and lay the foundation for new initiatives.

PART I: CSD PROGRAM ORIGINS AND BACKGROUND

Cold War Redux

As we gathered background information for this report, we noticed a pattern: experts and practitioners alike became quick to turn to the past for cues on how to proceed in the future. In fact, the discussion of the historical framework of disinformation as a threat area revealed a common understanding that the challenge of disinformation is “not new.” Several of our interlocutors spoke reverently of the tools of the Cold War and cited the merits of the United States Information Agency (USIA), Voice of America (VOA), Radio Free Europe/Radio Liberty (RFE/RL), and, most notably, the Active Measures Working Group (AMWG) as successful instruments of PD in countering disinformation.[2] However, these experts agreed that they might be over-emphasizing the similarities between the disinformation threat then and now, while perhaps unintentionally underestimating the differences.

Much of the apparatus that supported Cold War-era counter disinformation efforts still exists today, albeit in a somewhat disaggregated form. In 1999, USIA closed down as an independent foreign affairs agency. Its information, cultural, and exchange components were integrated into the Department of State as, respectively, the Bureau of International Information Programs (IIP) and the Bureau of Educational and Cultural Affairs (ECA). Meanwhile, oversight of USIA's regional programs was turned over to the State Department’s geographic bureaus. USIA’s broadcasting components became part of the Broadcasting Board of Governors (BBG–now the U.S. Agency for Global Media, or USAGM). The AMWG was formally disbanded in 1992 with no heir apparent; and at the BBG, the establishment of an independent board of directors removed direct USG editorial oversight and created a firewall between Congress and the independent journalism operations within the VOA and RFE/RL.

In addition to the structural changes that have occurred since the integration of USIA functions into the Department of State, the rapid convergence of connection technologies -- the internet, mobile and social networks -- have fundamentally altered the domain in which information

competition occurs. About half of the world's population has access to one another via the combination of internet and social media access and mobile phones, which allow for disintermediated peer-to-peer communication at scale. The global information space is marked by a constant fight for attention, and viewership is determined by complex interactions among algorithms, professional media outlets, corporate brands, and user generated content via apps on mobile devices.

As a consequence, modern public diplomacy practitioners find themselves in an environment that offers an overabundance of information—what Joseph Nye presciently described as a "paradox of plenty" that leads to a "scarcity of attention."[3] This shift has irrevocably changed the information environment in which PD officers operate, and it gives an asymmetric advantage to those who would attempt to alter, obscure, or destroy the very concept of objective truth.

> An overabundance of information…has irrevocably changed the information environment in which PD officers operate, and it gives an asymmetric advantage to those who would attempt to alter, obscure, or destroy the very concept of objective truth.

Initial efforts to meet the most recent iteration of these challenges began in the 2010s, during a period of what some have described as U.S. government "overexuberance" about the ability of emerging social media technologies to advance democratic values. By the time the Arab Spring began to unfold in 2011, new policies were established that encouraged State Department officials to establish online profiles and pages with the intent to amplify public affairs messaging through these increasingly influential mediums.

However, constrained by bureaucratic inertia and, perhaps, overconfident that "traditional" public diplomacy measures transposed to the online space (i.e., press releases, photos from speaking events and conferences, etc.) would have the intended effect, innovation on USG social media platforms largely stopped there. While these official Department social media accounts now number in the hundreds, most PD officials agree that for a number of reasons, including but not limited to the risk aversion that arises from engaging in an often-frenetic online environment, the overall impact remained relatively muted.

With the intensification of Russian disinformation efforts following Ukraine's "revolution of dignity" and the subsequent annexation of Crimea in 2014, it became increasingly clear that the social media space had become, in effect, the front line in a new global competition for influence. Shortly thereafter, the threat of disinformation expanded far beyond the borders of Eastern Europe to become the subject of intense focus from Washington, D.C. to the Silicon Valley. The 2017 National Security Strategy included a section on Information Statecraft warning about the exploitation of “marketing techniques.”[4] Meanwhile, Facebook CEO Mark Zuckerberg described efforts to combat disinformation on his platform as an “arms race,”[5] and Apple CEO Tim Cook warned that personal data was being “weaponized against us with military efficiency.”[6] To paraphrase Peter W. Singer, whose 2019 book *LikeWar*[7] explored this phenomenon in depth, tech executives were starting to sound more like national security experts, and national security experts were starting to sound more like tech executives.

With the intensification of Russian disinformation efforts following Ukraine's "revolution of dignity" and the subsequent annexation of Crimea in 2014, it became increasingly clear that the social media space had become, in effect, the front line in a new global competition for influence.

Recognizing a Resurgent State-Sponsored Disinformation Threat: 2016-2017

In the early stages of Russia’s attacks on Ukraine’s integrity in the global information space, the State Department’s Bureau of European and Eurasian Affairs (EUR) developed a nascent set of counter-disinformation tactics. But formal and far reaching alterations to PD CSD infrastructure originated with the passage of the May 2016 Countering Foreign Propaganda and Disinformation Act, which became a part of the 2017 NDAA. The first legislation tasking an official lead in government-wide counter-disinformation efforts since the Cold War, the NDAA signaled that the USG once again recognized disinformation as a high-priority threat that warranted immediate action.

The State Department’s GEC, established by Executive Order in March 2016, became the prime vehicle for CSD. It was originally envisioned as a mechanism to counter violent extremist (CVE) messaging and “foreign propaganda and disinformation” operations. However, the 2017 NDAA further charged the GEC with coordination and building capacities across the interagency as well as private sector partners and allies to combat state and non-state disinformation campaigns. The 2017 National Security Strategy crystalized the consensus that counter-disinformation work represented a key strategic priority, noting that:

> *America’s competitors weaponize information to attack the values and institutions that underpin free societies, while shielding themselves from outside information. They exploit marketing*

> *techniques to target individuals based upon their activities, interests, opinions, and values. They disseminate misinformation and propaganda. Risks to U.S. national security will grow as competitors integrate information derived from personal and commercial sources with intelligence collection and data analytic capabilities based on Artificial Intelligence (AI) and machine learning.*[8]

As a consequence of the NDAA and the National Security Strategy, a number of PD officers began to report back up the chain on disinformation threats in their regions. This new attention on the threat had a near immediate impact: cable traffic with the keyword "disinformation" at the State Department shows a 300 percent increase in the number of cables between 2017 and 2019; and a ten-fold increase in average monthly cable traffic between 2015 (8) and 2019 (81.5).[9]

However, this activity focused largely on generating awareness of the threat, rather than proposing or conducting actual responses to it. In 2017, 262 cables were sent mentioning disinformation, but few represented a concrete initiative or deliverable aimed at addressing the challenge. Instead, most focused on reporting on disinformation themes, or organizing conferences or speakers that would generate awareness of the threat.

Initial progress throughout 2017, therefore, remained mixed. Those interviewed by the ACPD described an increasing awareness of the disinformation threat through targeted educational, training, and outreach programs. However, they also outlined challenges – most notably, competing definitions about what constituted "disinformation," and an ongoing debate about what, if any, the U.S. government's role be in combatting it.

As such, in the earliest days after the formal establishment of the GEC, few agreed on what could or should be deployed to counter disinformation. Moreover, the GEC, in its previous incarnation as the Center for Strategic Counterterrorism Communication (CSCC), focused exclusively on efforts to counter violent extremism. The GEC and its staff had to figure out how to transition to its new disinformation mandate using resources, processes, and programmatic structures originally designated for its CVE mission.

The nascent GEC also encountered several structural barriers to effective execution of its mandate, some of which were

USG CSD efforts from 2016 to 2017 were generally more consumed with assessing and preparing to meet the resurgent state-sponsored disinformation threat, rather than actively engaging it.

entirely outside of the control of GEC leadership. First, the GEC launched in the midst of a year-long State Department-wide hiring freeze, which complicated the recruitment and staffing of those dedicated to the CSD mandate. This was followed by a funding freeze that delayed the disbursement of the congressionally allocated funding for GEC's CSD effort. Additionally, the absence of a permanent, confirmed Under Secretary for Public Diplomacy and Public Affairs ("R") for much of 2017-2018 meant that there was effectively no senior Department official to vouch for the GEC at a critical time for the roll out of its mandate. Finally, the proposed Department-wide "redesign" of 2017 raised questions about future roles and responsibilities of teams across the Department—to include the GEC.

Additional complications in the GEC's first year included those associated with structural transitions, such as the legal and operational restructuring of existing offices and roles to meet the new mandate, the establishment of new vehicles for contracting and resource acquisition, and the development of new working relationships and mechanisms with partner bureaus, the field, and the interagency.

Meanwhile, other elements of the wider public diplomacy community began to seriously engage on counter disinformation efforts. The BBG (USAGM), for example, prepared to launch its first new Russian-language satellite TV and digital network Current Time, in February 2017. Concurrently, VOA and RFE/RL launched the English and Russian-language fact-checking websites—Polygraph (2016) and Factograph (2017), respectively—to identify and report false or misleading information. Despite this new emphasis across the interagency, however, USG CSD efforts from 2016 to 2017 were generally more consumed with assessing and preparing to meet the resurgent state-sponsored disinformation threat, rather than actively engaging it.

Establishing CSD Priorities: 2018 - Present

Reinvesting in Long Term, People-to-People Engagement

In 2018, after about a year of assessment and preparation, activity began to ramp up considerably at the State Department with the finalization and funding of CSD proposals. Initially, much of the activity involved PD programming focused on long-term people-to-people engagement. ECA and, to a lesser degree, IIP – now part of the GPA – supported post-led initiatives such as workshops, exchanges, educational seminars, and speakers programs.

In July 2018, ECA took a big step forward in adjusting its programming specifically for CSD purposes when it was awarded a $12 million package to increase programming designed to counter Russian disinformation effects in the post-Soviet space. These new programs included a focus on improving media literacy, to include English language instruction with a media literacy component, capacity building and content support for local independent media outlets, cross-sectoral professional training and network development, and new successor generation outreach initiatives.

To prepare for an organized disbursement of these funds, ECA initiated a collaborative process in which it solicited input from other key stakeholders, including the GEC, the Bureau of European and Eurasian Affairs, the Bureau of South Central Asian Affairs (SCA), public affairs sections in the field, and interagency partners. Though not a recipient of supplemental funding, IIP also supported ECA's people-to people initiatives by making its existing programs such as the Speakers Program, American Spaces, Youth Networks, and Tech Camps available to posts that requested CSD support.

Beyond the strategic rationale for pursuing this initial CSD posture, there was another reason why IIP and ECA programs were so widely mobilized in response to the state-sponsored disinformation threat: they already represented some of the most well-understood and successful PD programs in the Department. Moreover, many PD officers in the field had already done a rotation through IIP or ECA, and virtually all had been briefed on their capabilities before deployment to their overseas assignments. As a result, these programs were among the most easily accessible to the field and relatively ready to transform and deploy quickly to boost posts' CSD footprint.

Acquiring and Developing New Tools and Techniques

The initial deployment of IIP and ECA resources in support of CSD initiatives followed long-established procedural and programmatic precedents. However, growing awareness of the digital nature of disinformation activities, enabled and empowered by big data and analytics, prompted internal efforts to update PD tools and techniques to meet emerging threats in the global information space. Initial attempts were made to identify every office or bureau with a stake in the response to computational propaganda, defined as a powerful weapon for spreading disinformation

> To be effective in this new threat environment, CSD program content and implementation would have to be synchronized across the board. No longer could affected bureaus and offices work in an independent, ad hoc manner on issues specific to separate regional and functional priorities.

that encompasses the now-familiar phenomenon of “bots” and “trolls.” Steps were also taken to identify programmatic vulnerabilities to computational propaganda and establish a basic nomenclature to facilitate collaborative responses. Finally, efforts were made to address the increasingly siloed nature of CSD programming within the Department of State.

Most significant, however, was the recognition that to be effective in this new threat environment, CSD program content and implementation would have to be synchronized across the board. No longer could affected bureaus and offices work in an independent, ad hoc manner on issues specific to separate regional and functional priorities, especially given the need to maximize program efficiencies and reduce the risk of compartmentalization. As awareness of the digital threat grew across the Department, DOS bureaus and other USG agencies including the GEC, IIP, and the BBG (USAGM) rapidly began to build new teams with capabilities that could soon be deployed at scale. The early effort to identify and describe roles in countering digital disinformation also proved to be useful in elevating the issue to more senior officials and generating a genuinely collaborative interagency conversation.

In the first half of 2018, IIP started to scale its analytics effort to meet emerging digital challenges. Initially made up of just a handful of analysts handling ad-hoc questions on social media engagement, the team began to field a stream of queries on issues ranging from digital marketing to strategic planning, measurement, focus groups, and a wider array of consultative services. Many of the requests touched on the topic of disinformation. To meet these rapidly growing challenges to the effectiveness of PD programming, the Office of Analytics expanded, adding specialized personnel and acquiring new tools and technologies to better understand and engage in digital information environments. The team also began to coordinate with content producers, helping meaningful content reach priority audiences. By the end of 2018, IIP’s new analytics team had grown significantly, incorporating several dozen specialists to cover major aspects of both behavioral and information science disciplines. About half of IIP’s analytics requests supported the GEC’s nascent counter-disinformation initiatives during this time.

Concurrently, the GEC was working to secure new resources and personnel that would enable it to fulfill its mandate as coordinating mechanism and "force multiplier" of U.S. government and partner efforts to counter state and non-state disinformation activities.[10] In February 2018, the Department of State announced that it had reached an agreement with the Department of Defense (DoD) to transfer a maximum of $40 million to the GEC to fund "counter propaganda and disinformation from foreign nations."[11] This became the GEC's primary source of funding as outlined in the 2017 NDAA. Although the initial amount transferred represented only half ($21.1 million) of the total requested, it was nonetheless critical to GEC's efforts. In FY2018, GEC's CSD funding totaled $41.1 million, meaning that 49 percent of its CSD operations were dependent on DoD, but they were wholly GEC-led and added a significant new element to the Department of State CSD programming mix.[12]

In May 2018, Secretary of State Pompeo lifted the Department-wide hiring freeze that had been in place since the GEC's establishment.[13] In the second half of 2018, with funding from DoD acquired and the DOS hiring freeze lifted, the GEC finally began to take shape. First, the GEC restructured its offices into four threat-based teams: [14]

- The **Russia Team** focuses on understanding, opposing, and degrading Russia's global implementation of information confrontation through leadership of policy, programmatic, and analytic efforts across the USG interagency and with foreign partners. The team works with EUR, DoD's European Command, and several foreign partner governments to identify vulnerabilities and needs, and to synchronize and deconflict programs and other efforts. In 2019, in addition to its continuing focus on Europe, the Russia Team expanded its programming, particularly in Latin America.

- The **China Team** has designed a global strategy to counter Chinese Communist Party (CCP) disinformation and propaganda efforts. This strategy aims to 1) boost understanding of CCP propaganda and disinformation to promote informed decision making; 2) build resilience to disinformation and propaganda with programs that develop a more robust and more capable civil society and media; and 3) support content development and amplification of positive USG messaging. The China team coordinates with the Bureau of East Asian and Pacific Affairs, the Deputy Secretary's office, and other State Department bureaus. The team also works closely with the interagency, including the DoD, and international partners.

- The **Iran Team** coordinates the U.S. government's interagency efforts to counter disinformation and propaganda inside and outside of Iran, assisting partners to expose the Iranian regime and ensure that partners have the latest assessments and analytics to support USG interests.

- The **Counterterrorism Team** focuses on the expansion and integration of international, regional, and national networks of partners who can assist in rolling back the counterfactual narratives of terrorist organizations and their affiliates, engage vulnerable audiences, and deny the adversary's recruitment and radicalization objectives. The team identifies best practices for the innovation and rapid deployment of audience analysis, grievance mapping, content generation, and monitoring and evaluation of impacts and other data analytics tools.

Next, GEC supported these teams through establishing several lines of effort:

- The **Analytics & Research (A&R) Team** uses quantitative analysis (with context-specific qualitative input) to provide actionable insight to address disinformation and propaganda and shape strategic communication efforts. A&R, which originated in 2018, is a multi-disciplinary team, including data scientists, statisticians, intelligence analysts, strategic communications professionals, and geopolitical subject matter experts.

- The **Information Access Fund (IAF)**, established at the end of FY2018, allows for an open, competitive grant application process for outside public and private organizations interested in CSD activities. Applicants include civil society groups, media content providers, nongovernmental organizations, federally funded research and development centers, private companies, and academic institutions. Proposals are solicited in four major thematic areas:

  a. Support for foreign independent media best placed to refute foreign disinformation in their own communities;

  b. The collection and storage of foreign disinformation, misinformation, and propaganda targeted at the U.S. and its allies;

  c. The analysis of and reporting on the latest tactics, techniques, and procedures of foreign information warfare; and

  d. Support for other GEC activities.

Other major initiatives funded by the initial tranche of IAF funding in 2018 include support for the study of disinformation using data mining and computational analysis at major U.S. universities for the purpose of development of independent media abroad and the establishment of fact checking organizations.

- The **Technology Engagement Team (TET)** originated in 2018 as an interagency group focused on the identification of technological solutions and the development of public-private partnerships in the fight against foreign propaganda and disinformation. Today, TET convenes technology experts and programmatic authorities from the public and private sectors to identify, assess, test, and implement technologies against the problems of foreign propaganda and disinformation, in cooperation with foreign partners, private industry, and academia.

Its programs include the Washington-based Tech Demo Series, overseas Tech Challenges, a technology Testbed, and its information repository at Disinfo Cloud.

- Under the **Policy, Plans and Operations Division (PPO)**, the International and Interagency Coordination Cell (I2C2) links interagency and international partners to accelerate responses to adversary propaganda and disinformation. The I2C2 is responsible for building and maintaining a network of interagency, international, private, civil society, tech industry, media, and private sector partners. It also includes a Network Engagement and Training Cell that cultivates partnerships with foreign civil society, advocacy, communications, and other networks to build on and leverage counter disinformation capabilities.

Mobilizing and Deploying Resources

From 2016 to 2018 the "R" family, including the Office of Policy, Planning and Resources (R/PPR), IIP, ECA and GEC, steadily pivoted toward new disinformation-focused PD capabilities. However, the deployment of these initiatives in the field took place at the discretion of the regional bureaus, which, to this day, have the authority to adjust resource allocations and program implementation to meet specific field level needs, or account for constraints imposed by local operating environments and bilateral policy priorities. As a consequence, approaches to countering state-sponsored disinformation effects have varied significantly from region to region and even post to post.

While each regional bureau coordinates digital support for the field, EUR went a step further, establishing a standing StratCom unit in 2018. EUR StratCom served as a line of coordination with the field on priority PD topics, including articulating the bureau's overall CSD posture and goals. In 2018, StratCom tasked each post in EUR to develop a custom CSD plan, and region-wide workshops were held to generate awareness and discuss best practices among embassy teams, including PD officers. By mid-2018, most missions in Europe had formulated a CSD strategy.[15] As these CSD coordination efforts gained traction within the regional bureaus and additional R family resources became available, the range of new tools, expertise, and capabilities began to expand. This marked the beginning of a period of Department-wide experimentation with approaches to CSD.

In addition to resource and programmatic challenges, one of the most significant barriers to the successful implementation of CSD programming is the lack of social media outreach expertise among PD practitioners. The National Foreign Affairs Training Center (NFATC), home of the State Department's Foreign Service Institute (FSI), has emerged as one of the major stakeholders in mitigating the widening digital education gap. Over the past few years, FSI, which prepares Public Diplomacy officers for deployment to the field, has significantly revised its training modules to address the tools and techniques required to function effectively in the global information space. Former FSI PD Training Director Will Stevens described the need for change in 2017:

> *When we talk about public diplomacy training, we need to talk about the tectonic shifts that are happening in influence environments all over the world...Instead of having sages tell old war stories, what we're doing is we're teaching people skills and then immediately giving them a chance to try to apply them. Immediately having them practice and practice again and practice again in different environments, so that they have the chance to actually solidify that knowledge...Twitter is different today than it was six months ago, much less, you didn't even learn about Twitter when you went to the FSI course on how to be a press officer a decade ago. So how do I get that training to you in the field in a way that helps you when you need it? And that means directly partnering with our colleagues in IIP, in ECA, making sure that we're getting [training] to people when they need it.*[16]

Since 2017, FSI PD training has shifted to focus on modules of data literacy, audience segmentation, landscape analysis, strategic narrative development, measurement and evaluation, and program management. As recently as April 2020, FSI was conducting a needs assessment for developing a course specifically to address foreign disinformation and propaganda campaigns.

> When we talk about public diplomacy training, we need to talk about the tectonic shifts that are happening in influence environments all over the world...Instead of having sages tell old war stories, what we're doing is we're teaching people skills and then immediately giving them a chance to try to apply them.

New Beginnings for Legacy PD Apparatus

By the end of 2018, new capabilities to counter state-sponsored disinformation were established and implemented across the Department and much of the wider PD community, and they would soon be supported by two high-profile changes to the legacy PD apparatus: the restructuring of USG broadcasting services into USAGM and the creation of GPA at the State Department.

U.S. Agency for Global Media

The USAGM has its institutional antecedents in the BBG, which was established through the International Broadcasting Act of 1994. Embedded within the USIA, the BBG supervised all non-military broadcasting services, to include five full-scale, global media networks across 100 countries, and produced programming in 61 languages. In 1999, the BBG became a standalone agency when USIA merged into the Department of State.

With a FY2018 budget of over $800 million and a full-time staff of more than 1,400, the BBG was, historically, the single largest element of USG PD infrastructure. However, despite its scale and resources (and perhaps, in a sense, because of them) the BBG struggled to meet the challenges presented by the contemporary media environment. As a consequence, in an August 2018 tweet, BBG CEO John Lansing announced a formal organization-wide restructuring, complete with the re-naming of this legacy PD organization, citing a global media environment and "weaponized information" as a rationale:

> *The U.S. Agency for Global Media [USAGM] is a modern media organization, operating far beyond the traditional broadcast mediums of television and radio to include digital and mobile platforms. The term "broadcasting" does not accurately describe what we do...USAGM is an independent federal agency that provides accurate, professional, and objective news and information around-the-globe in a time of shifting politics, challenging media landscapes, and weaponized information. Our identity and name will now address these realities.*[17]

To this end, the newly-renamed USAGM worked to develop the technological and analytical capabilities now standard in a modern, integrated news media operation. For example, it began investing more in digital and mobile communications such as short, shareable video content geared for mobile consumption, and worked to build out a nascent analytics capability with new digital media specialists. To implement more data-driven decision making into the overall workflow, a Chief Strategy Officer position was established.

Early signs of the transformation included the deployment of cloud-based dashboards in the newsroom, which allow for real-time performance measurement. USAGM reports that the re-focusing of efforts toward digital communications has yielded notable early results: views on YouTube for FY 2017 increased across the board, with RFE/RL reporting a 72 percent increase in content viewed; Radio Free Asia's Cantonese Service reported a 792 percent increase; and VOA reported percentage gains in the "triple-digits" on Facebook video engagement.[18]

While this is encouraging and signals an important shift toward more effective communication in a complex media environment, it still remains a relatively small investment from such a large institution. Moreover, the vast majority of USAGM operations still rely on traditional broadcasting and radio formats. A 2019 report[19] commissioned by USAGM found, for example, that the Office of Cuba Broadcasting (OCB)'s Radio and TV Marti ineffectively engages Cuba's emerging youth population. Built for linear radio and TV production, the OCB's current operating structure and professional expertise remain fundamentally misaligned with the informational needs and technological sophistication of Cuba's emerging and influential youth citizenry. The report recommended a wholesale modernization of the network, to include streamlining operations and relaunching as a digital first and agile news service to provide highly engaging content.

While large scale change takes time, USAGM has made a concrete effort to address state-sponsored disinformation. The 2017 launch of the Russian-language satellite and digital network Current Time represents the most important of USAGM's CSD initiatives. According to USAGM, this joint effort by RFE/RL and VOA provides "Russian-speakers...with access to accurate, topical, and trustworthy information," and "serves as a reality check on disinformation that drives conflict in the region." Available via satellite and local distributors in 20 countries (an additional 15 countries carry specific programming), the network is also, importantly, amplified by a digital division that engages audiences through an internet-friendly content mix that includes short videos, longer-form explainers, quizzes, and entertainment.

Since its launch, the Current Time network has expanded rapidly, and USAGM reports that CT's digital content – video in particular – has been key in driving its growth. In 2018, digital video on the network garnered 500 plus million views online and across social media platforms; one million plus followers across social media platforms; 900,000 plus followers on the network's primary Facebook page; and 600,000 plus subscribers on YouTube. Perhaps most interestingly (and uniquely) for USAGM, Current Time's digital platforms have acquired regular engagement from a key, growing demographic – a millennial-aged audience. According to data provided by USAGM, 45 percent of Current Time engagements are from users under 35 years of age, and many are returning readers; the network averages of 160,000 daily engaged users on Facebook alone.[20]

However, there continue to be significant budgetary constraints. Even as USAGM made the transition to digitally-focused operations, Current Time operated on a $17 million budget--just two percent of USAGM's then $800 million operating budget. Polygraph and Factograph, USAGM's fact-checking websites, have resources even smaller than that. By contrast, adversarial outlets have had exponentially greater resources to draw from. For example, in 2017 the global media network Russia Today (RT) had an estimated operating budget of $323 million.[21]

Despite these challenges, the top-down re-imagining of how this sprawling, legacy PD organization can operate in the global digital environment has shown signs of success. Continued experimentation with new technology and platforms has the potential to increase engagement directly with foreign audiences that may be otherwise susceptible to disinformation in a way that few other existing PD programs can replicate. As a May 2020 USAGM report on countering disinformation concludes, some very good progress has been made in recent years, but more can be done. Specifically, the report recommends improving content production to meet digital outlet best-practices (i.e., user-generated content, live streaming); leveraging distribution to reach target populations on their preferred devices/mediums; expanding cooperation with trusted local partners/messengers; and expanding fact-checking efforts.[22]

Bureau of Global Public Affairs

The May 2019 formation of GPA occurred in response to dramatic and accelerating changes in the global information environment, to include the malign influence threat. The merger of PA and IIP was designed to permit more effective communication in the digital world, integrate existing capabilities, increase collaboration and impact, and deliver on Department communications objectives, both foreign and domestic. The new structure was intended to integrate the communication of official Department policies, previously the purview of PA, with creative, data-driven content and storytelling around American values, as originally produced by IIP.

As part of this merger, several entities from PA and IIP not aligned with the core communications capability transitioned to other public diplomacy and training bureaus within the Department where they would be best optimized. The American Spaces, U.S. Speaker, and TechCamps programs joined ECA to bring together people-to-people functions. Meanwhile, IIP's regional and functional policy liaisons, judicial liaison, networks team, the ACPD Secretariat, and PA's U.S. Diplomacy Center (renamed the National Museum of American Diplomacy in November 2019) staff moved to the R Bureau's R/PPR to consolidate strategic planning, capacity development, and resource-to-policy alignment. Finally, the Office of the Historian joined the Foreign Service Institute to integrate the Department's research initiatives and archival resources.

Described as "the biggest structural change at the State Department in 20 years," the new bureau was also intended to be "part of a broader effort to counter disinformation campaigns by Russia and China."[23] At an ACPD event in September 2019, former Assistant Secretary for Global Public Affairs Michelle Giuda noted that the new bureau would be leveraging its new analytics capabilities in tandem with its messaging to monitor and pre-empt disinformation as it happens:

> *We know the news cycle is moving instantaneously, so we must work quickly...to get our message out, to make sure that the truth is out there before some counter-narratives from other folks out there in the world...[We also need to be effective in communicating] our values over time.*[24]

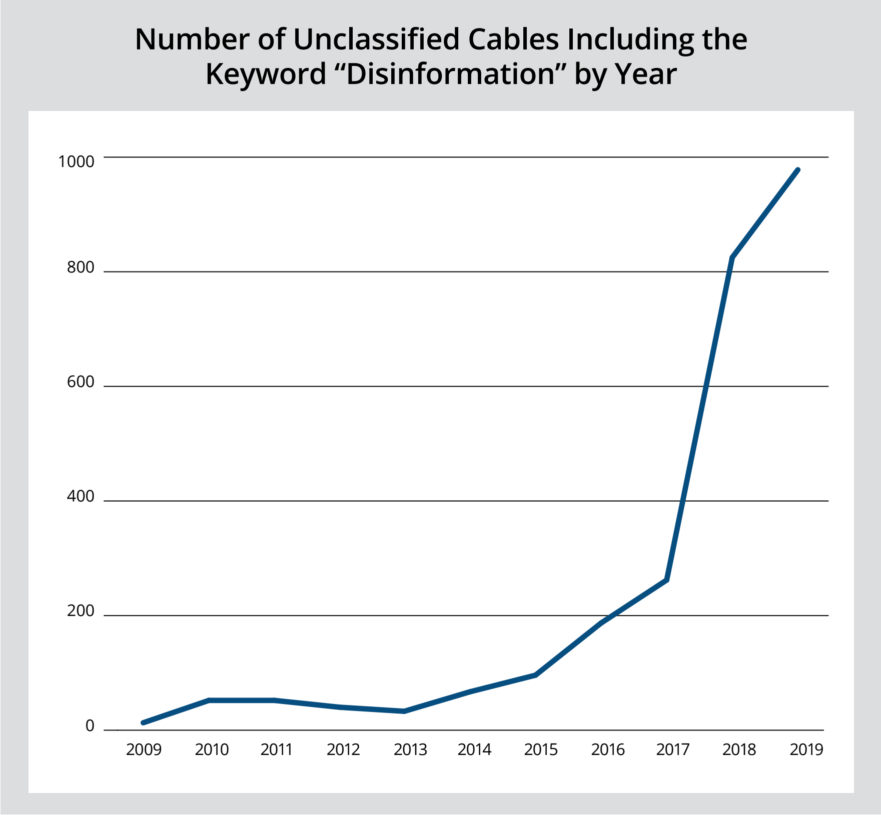
It remains to be seen whether the configuration of information and outreach initiatives under the GPA will prove to be more effective in countering malign influence effects than its institutional predecessors.

PART II: CSD PROGRAM REVIEW AND DIAGNOSTIC

To obtain a diagnostic overview of counter state-backed disinformation activities across the USG PD community, the ACPD ran three separate data collection efforts: a review of unclassified cables with the keyword "disinformation" (2009-2019); a keyword search of State Department country and functional bureau strategy documents (2018); and a survey of field-based PD practitioners on "Countering State-Sponsored Disinformation" (May 2019). Note that data tagged as "regional" originates from posts in specific geographical regions rather than from the Washington-based regional bureaus.

Dataset 1: Unclassified State Department Cable Traffic

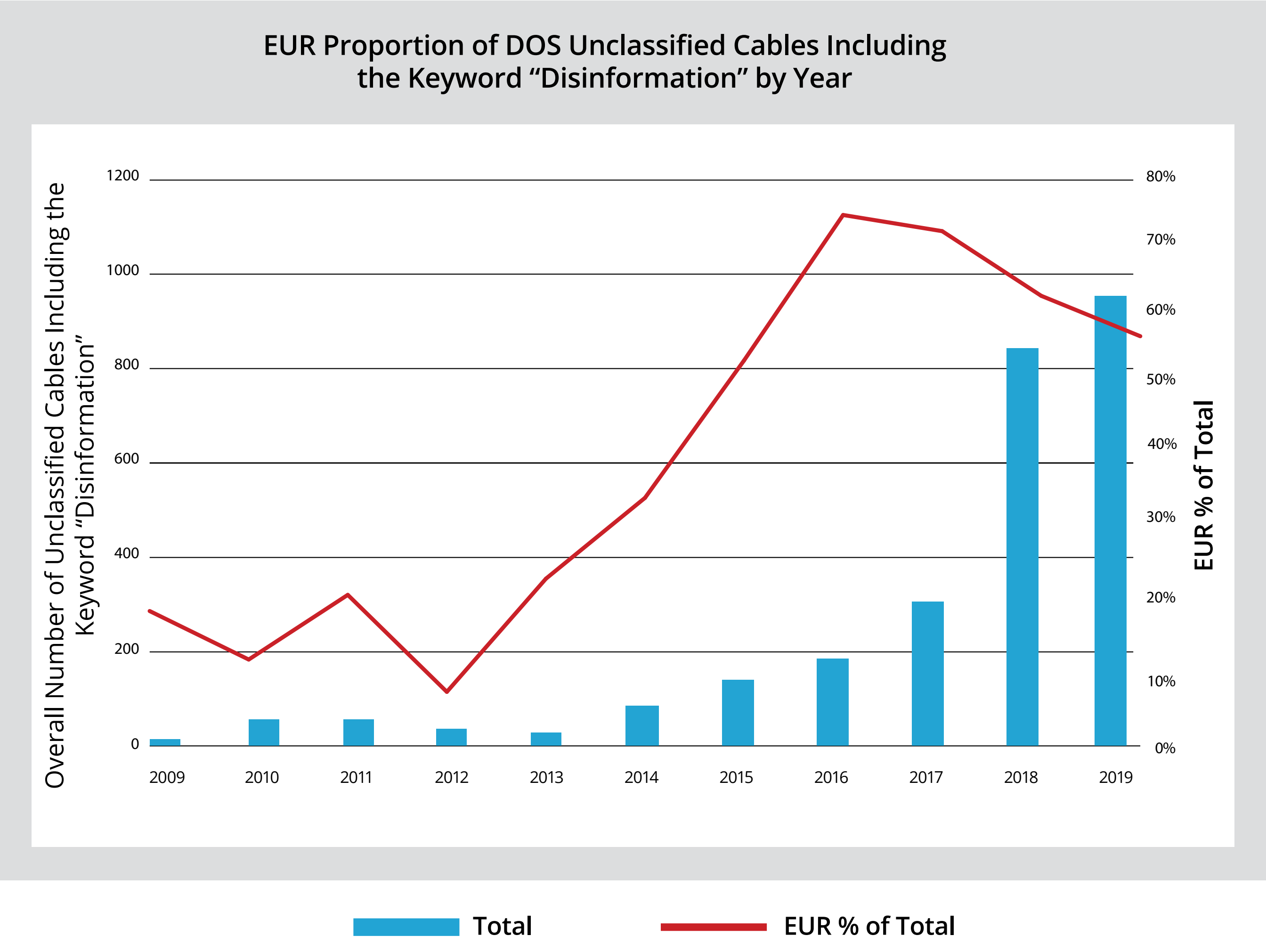
Graph A: *Number of Unclassified Cables Including the Keyword "Disinformation" by Year*



The ACPD collected data on all unclassified State Department cables that mentioned the keyword "disinformation" over the last eleven years. As Graph A indicates, in 2009, the word "disinformation" was found just 13 times in the entire calendar year (CY). From 2009 forward, the number of cables mentioning the word increased by an average of 27 percent per year, with the largest single year jump in cables between 2017 (262) and 2018 (825). That number increased again in CY 2019, approaching nearly 1,000 cables.

Graph B: *EUR Proportion of DOS Unclassified Cables Including the Keyword "Disinformation" by Year*

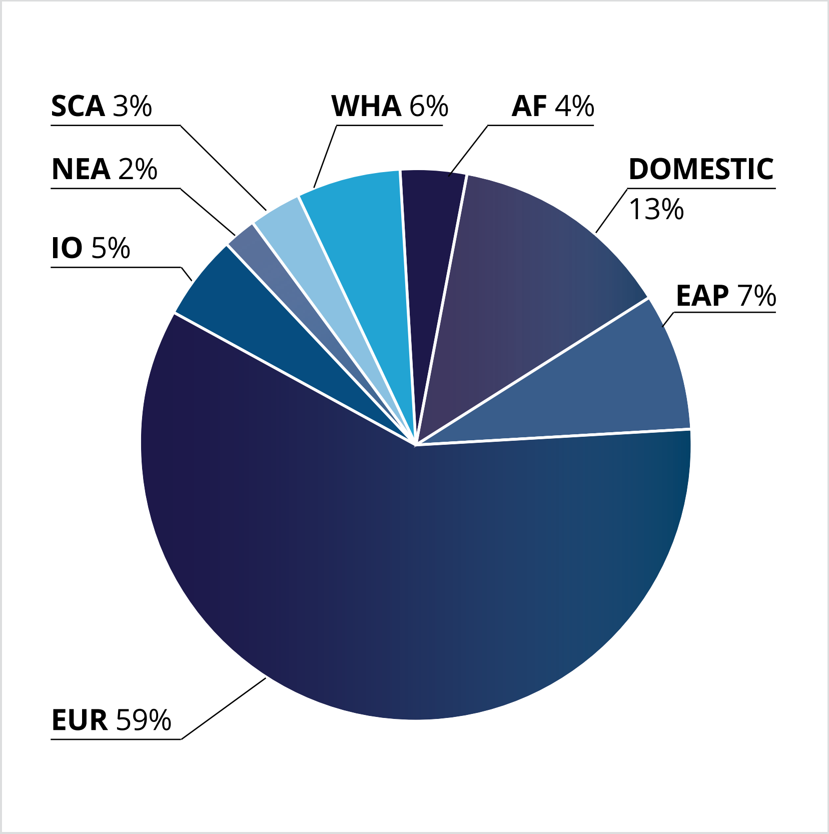
In recent years, cables originating in Europe and Eurasia (EUR) accounted for a significant and growing proportion of overall cable traffic on the subject of disinformation. Roughly tracking increased Russian activity in Eastern Ukraine and Syria, EUR cable traffic spiked from 13 percent of total DOS unclassified cable traffic mentioning “disinformation” in 2012 to a high of 72 percent in 2016. However, beginning in 2017, other regions appeared to have turned their focus to the disinformation threat, and EUR’s percentage began to decline as overall cable traffic on CSD increased. As seen in Graph B, cable traffic from the other six regions mentioning the keyword “disinformation” surged by over 700 percent between 2016 (52) and 2019 (423). Meanwhile, the proportion of traffic originating in EUR that mentioned “disinformation” declined 13 percent over that same period, from 72 percent in 2016 to 57 percent in 2019.



Graph C: *Regional Breakdown of Unclassified DOS Cable Traffic Including the Keyword "Disinformation" in CY 2019*

Perhaps indicating increased interest from Washington, many of the non-EUR cables mentioning disinformation did not originate from the field and were labeled as "Domestic" or Washington-origin traffic. In 2016, cable traffic including the keyword "disinformation" and labeled "Domestic" numbered only 11, but by 2018, 85 domestic cables mentioned the keyword. As shown in Graph C, "Domestic" was second in overall traffic origin in 2019, behind EUR and ahead of East Asia and the Pacific (EAP).

Regional Breakdown of Unclassified DOS Cable Traffic Including the Keyword "Disinformation" in CY 2019



Regions

AF: Africa

EAP: East Asia and the Pacific

EUR: Europe and Eurasia

IO: International Organizations

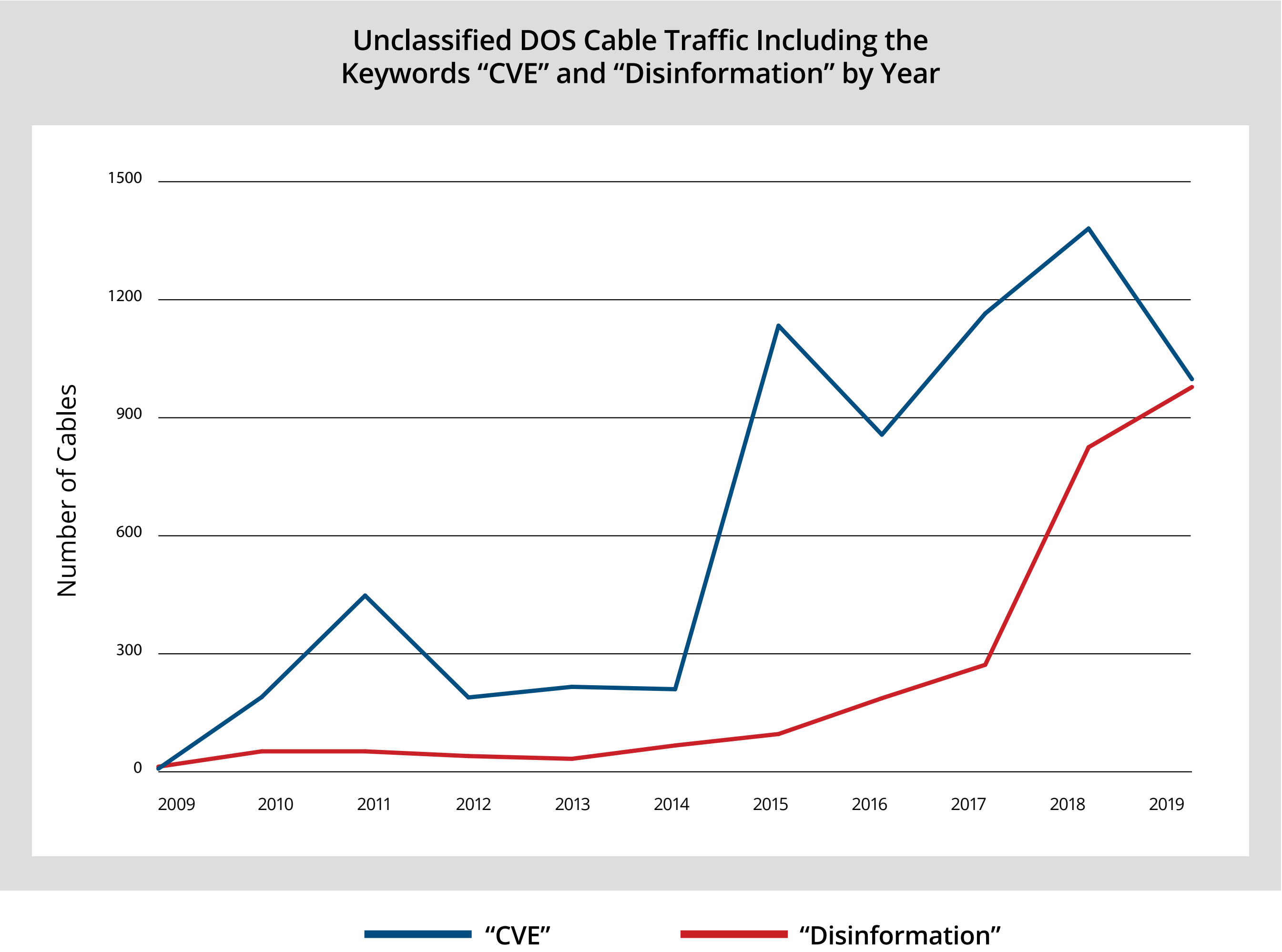
NEA: Near East Asia

SCA: South and Central Asia

WHA: Western Hemisphere

Graph D: *Unclassified DOS Cable Traffic Including the Keywords "CVE" and "Disinformation" By Year*

The scale of the numbers suggests that in this period the Department of State directed a historic amount of attention at the global disinformation threat. For context, we have compared the number of cables over the same eleven-year period with the theme "Countering Violent Extremism (CVE)." As Graph D demonstrates, the number of cables including the keyword "CVE" outnumbered those including "disinformation," but that gap has almost entirely closed. By the end of CY 2019, "CVE" yielded 998 search hits, while "disinformation" yielded 978.

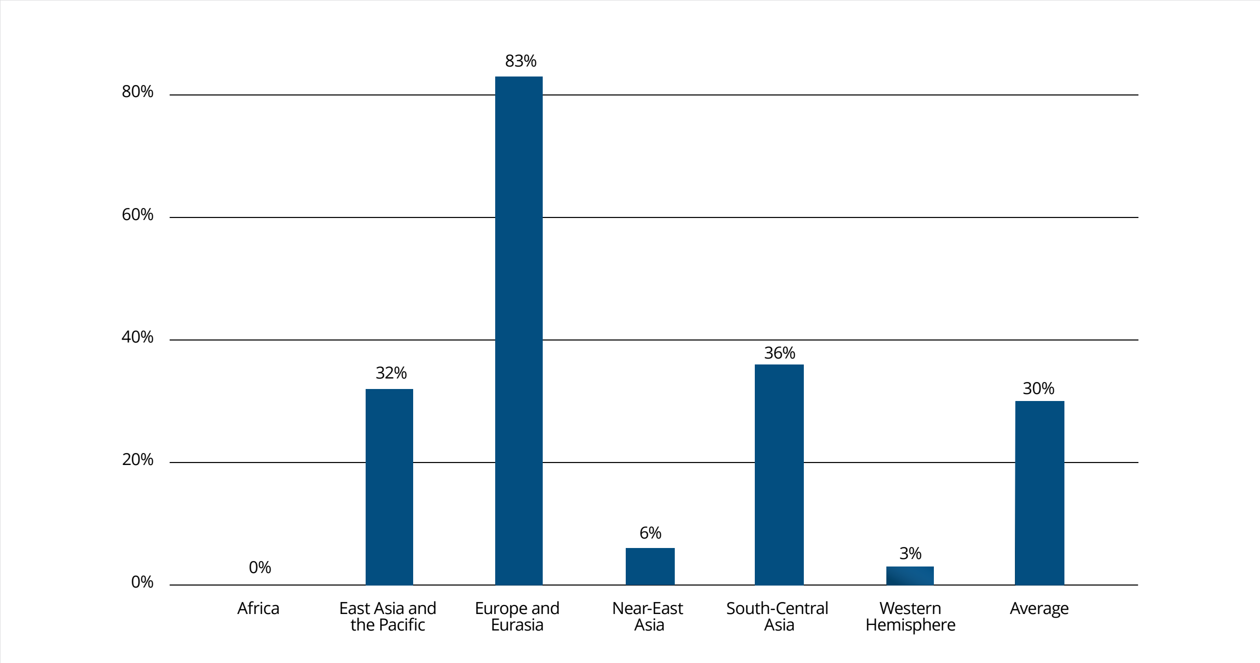


Dataset 2: 2018 Integrated Country Strategy and Functional Bureau Strategy Documents

Graph E: *Regional Breakdown of ICS Including the Keyword "Disinformation"*

The ACPD ran keyword searches in all of the 175 available 2018-2019 Integrated Country Strategies (ICS), as well as 41 available Functional Bureau Strategies. These DOS planning documents articulate U.S. strategic priorities in a given country, and for the Department's functional areas, such as arms control or environmental policy. Unfortunately, several Regional Bureau Strategies were not available at the time of writing and thus were not included in this dataset. Working with available data, we found that most posts in EUR mentioned counter disinformation programming as a priority in their respective country strategies, but that in other regions the numbers dropped significantly.

Regional Breakdown: Percentage of Available ICS Including the Keyword "Disinformation"



The ACPD also looked at 41 Functional Bureau Strategies available for review. Only five mentioned "disinformation" in their most recent strategy document at the time of writing. They were: PA; ECA; GEC; Democracy, Human Rights and Labor; and Arms Control, Verification and Compliance.

Dataset 3: Post-Led Counter-Disinformation Activities

In May 2019, the ACPD partnered with the GEC to conduct a survey with field-based PD practitioners. In consultation with the ACPD, the GEC established the data call parameters. The data call requested that all posts worldwide provide data on USG CSD activities that met the following criteria:

- The activity was unclassified;
- It was initiated between January 2017 and May 2019 (the date the data call request was approved and disseminated);
- Countering state-sponsored disinformation is/was the primary strategic purpose;
- Post executed the program directly, obligated the funding, or initiated it with a Washington bureau for support; and
- It included any program that was conducted regionally or in collaboration with other posts.

Additionally, the ACPD and GEC directed posts to include only grant activities awarded directly by post.

Graph F: *Post Responses to CSD Program Survey Sorted by Region*

The ACPD received responses from 44 posts representing 34 missions around the world, as shown in Graph F. Out of a total of 166 missions worldwide listed at usembassy.gov at the time of publication, this reflected a mission response rate of about 20 percent.

Regions

AF: Africa

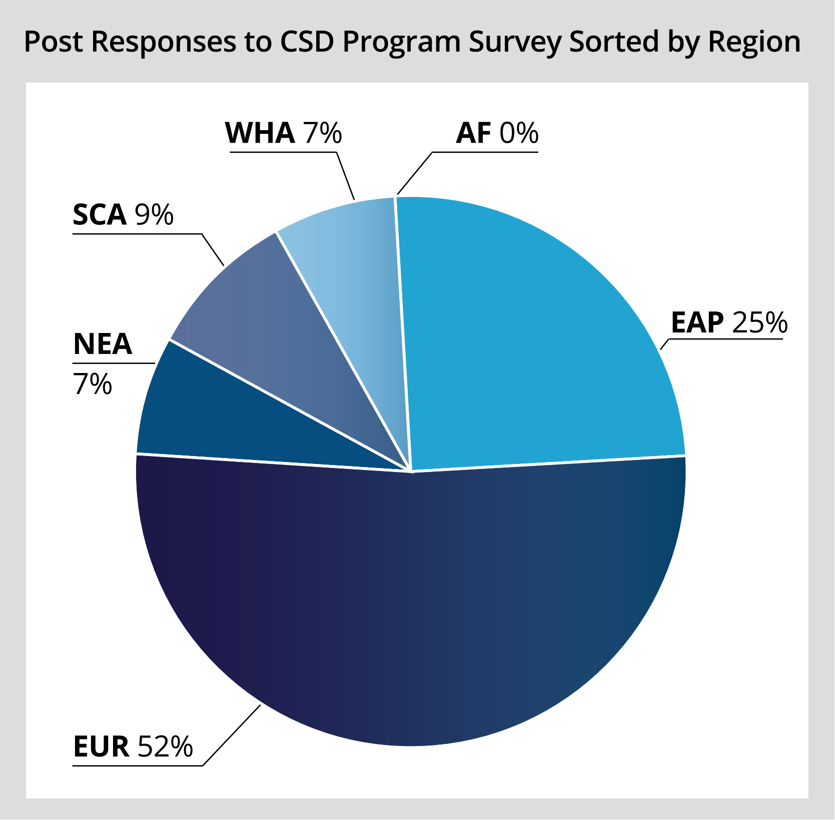
EAP: East Asia and the Pacific

EUR: Europe and Eurasia

NEA: Near East Asia

SCA: South and Central Asia

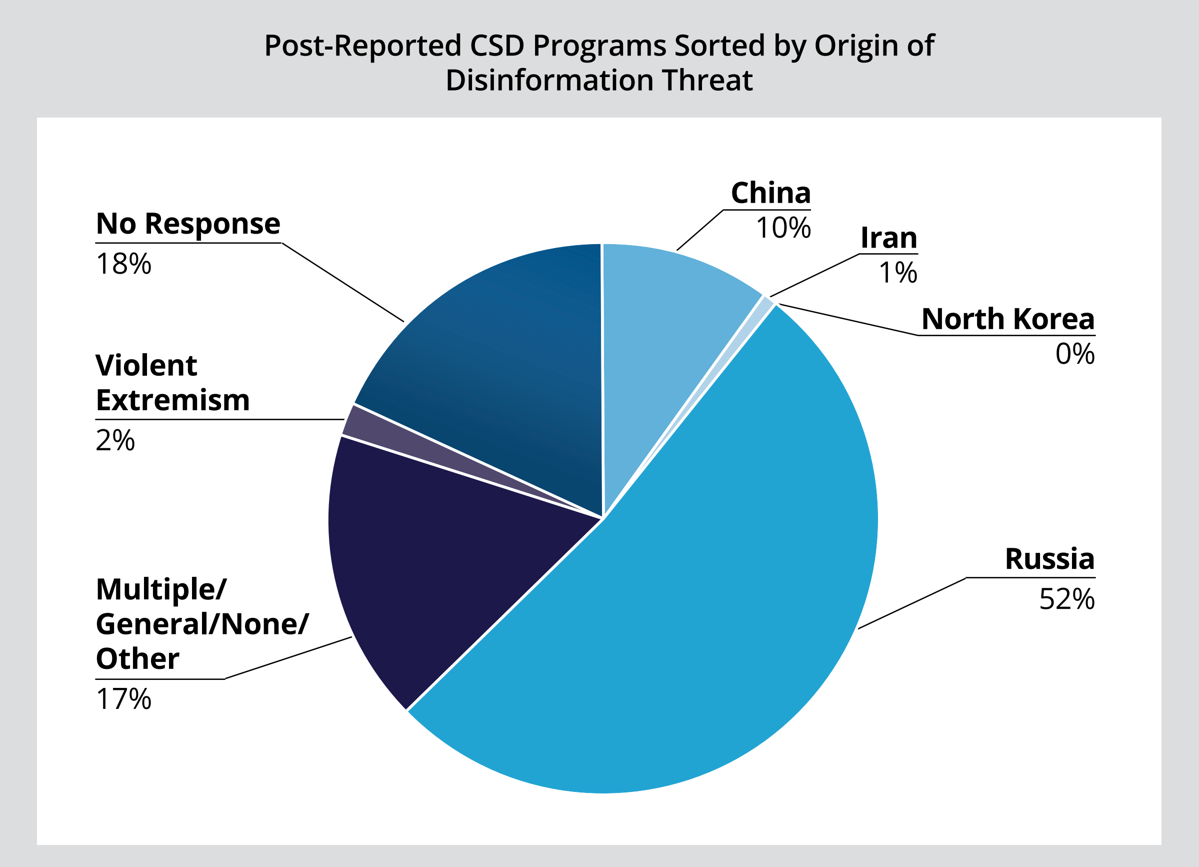
WHA: Western Hemisphere



Graph G: *Post-Reported CSD Programs Sorted by Origin of Disinformation Threat*

The missions that responded reported a combined 367 individual CSD programs initiated in the preceding 27-month period. These responses, together with data gleaned from relevant cable traffic and the ICSs, indicated that most CSD activity occurred at European posts. In fact, over 50 percent of the responding posts and nearly two-thirds of the number of individual programs reported were in the EUR region.

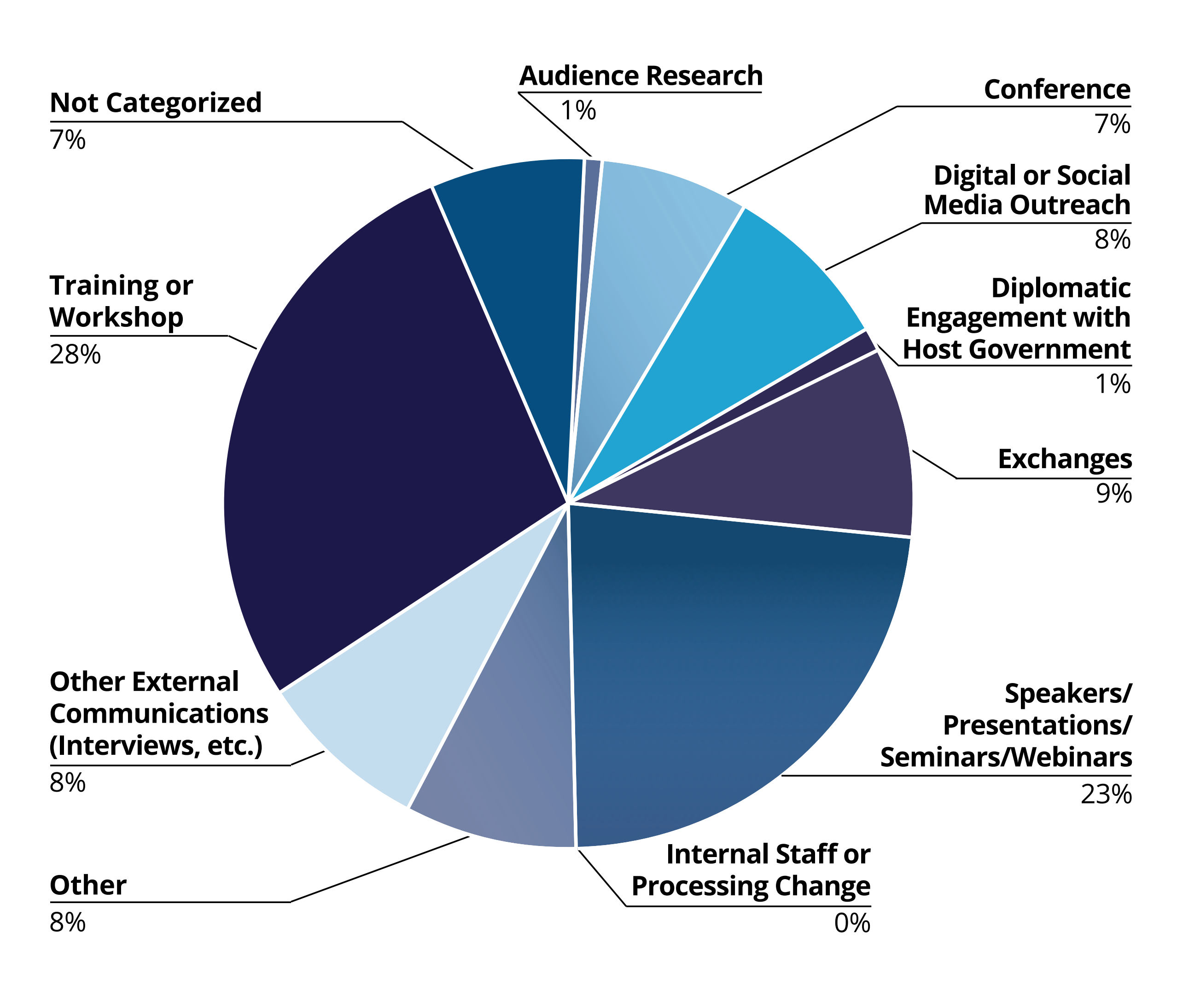
Not surprisingly, given the disproportionate number of responses coming from EUR posts, Graph G illustrates that activities directed at countering Russian disinformation accounted for 52 percent of the programs reported in the data call. The second and third largest groups of responses—a combined 35 percent—had an indistinct or unspecified threat actor: 17 percent reported "Multiple," "General," "None," or "Other," and 18 percent reported "No Response." This may indicate either a reluctance on behalf of a post to attribute their program to a specific threat actor, or the inability to narrow the program goal to focus on a specific disinformation threat. In either case, this suggests that PD CSD programming has frequently been, by design or not, more generalized than threat-specific. Another explanation for low response rates in some regions could be competing bureau definitions of malign influence activities, including disinformation.



Graph H: *Post-Reported CSD Programs Sorted by Activity Type*

In the survey, posts were given a wide range of GEC-defined activity categories to report on. The results depicted in Graph H show that various forms of direct person-to-person interaction of an educational nature, such as exchanges or training workshops, were, by far, the most frequently reported type of program. Taken together, the following activity types represented more than two-thirds of programs reported: conferences (7 percent), exchanges (9 percent), speakers, (23 percent) and training events (28 percent). By comparison, activities that occurred primarily in the digital space that had the potential to reach larger audiences comprised only 8 percent of the responses.

Post-Reported CSD Programs Sorted by Activity Type

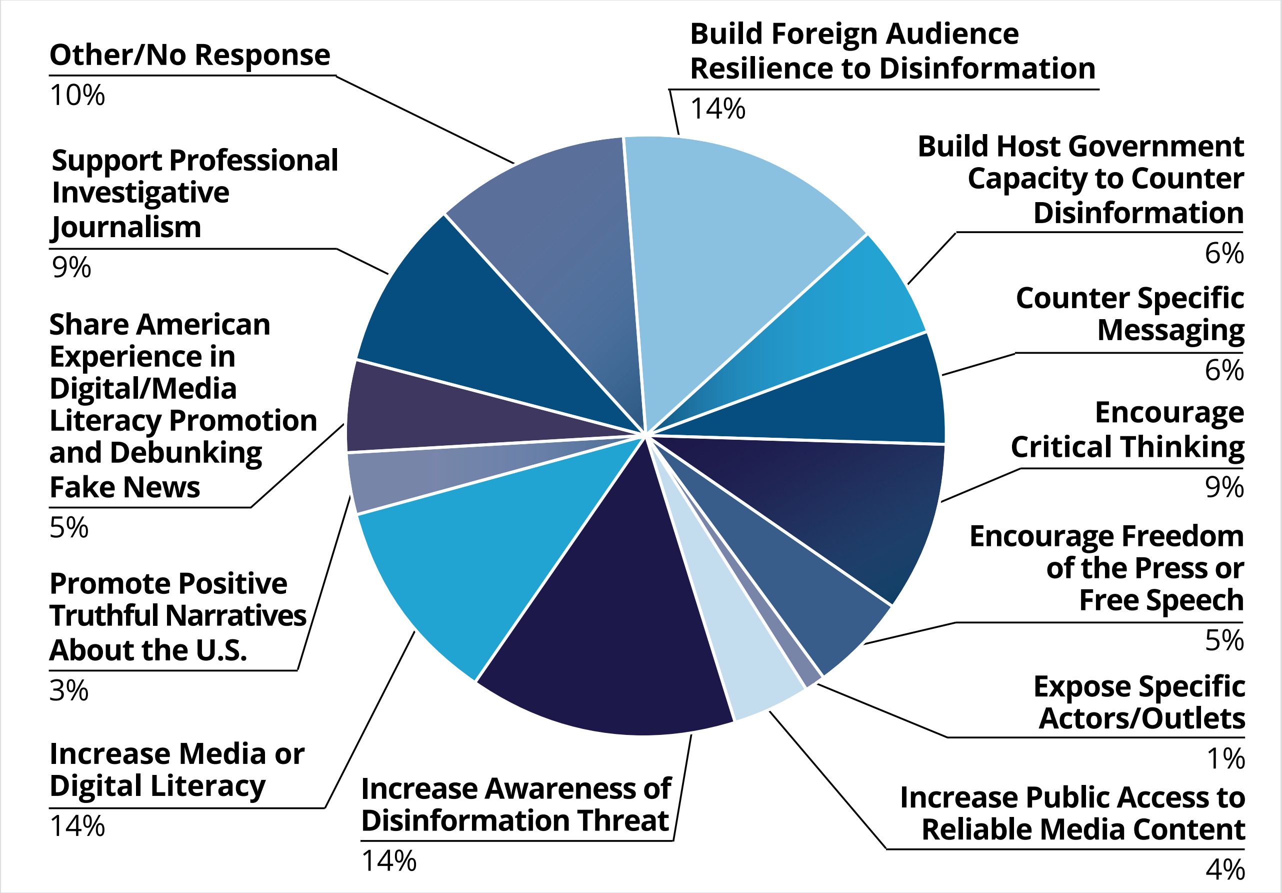


Graph I: *Post-Reported CSD Programs Sorted by Primary Objective*

Posts were also given a menu of GEC-defined program objectives to choose from, as well as a write-in option. As shown in Graph I, these objectives were more evenly dispersed compared to the other categories of the data call. However, a combined 75 percent of programs were designed to support long-term capacity building or resilience efforts: 9 percent supported "professional investigative journalism"; 6 percent bolstered host government capacity; 4 percent aimed to increase "public access to reliable media content"; 14 percent supported "foreign audience resilience to disinformation"; 9 percent encouraged critical thinking; 5 percent promoted freedom of the press; 14 percent aimed to "increase awareness of the disinformation" threat; and 14 percent addressed media or digital literacy.

A comparatively small proportion of programming—just 15 percent—was aimed at actively countering current narratives that were already impacting the information environment: 3 percent promoted "positive truthful narratives" about the United States; 1 percent exposed specific actors/outlets; 5 percent shared "American experience in debunking fake news"; and 6 percent countered specific messaging.

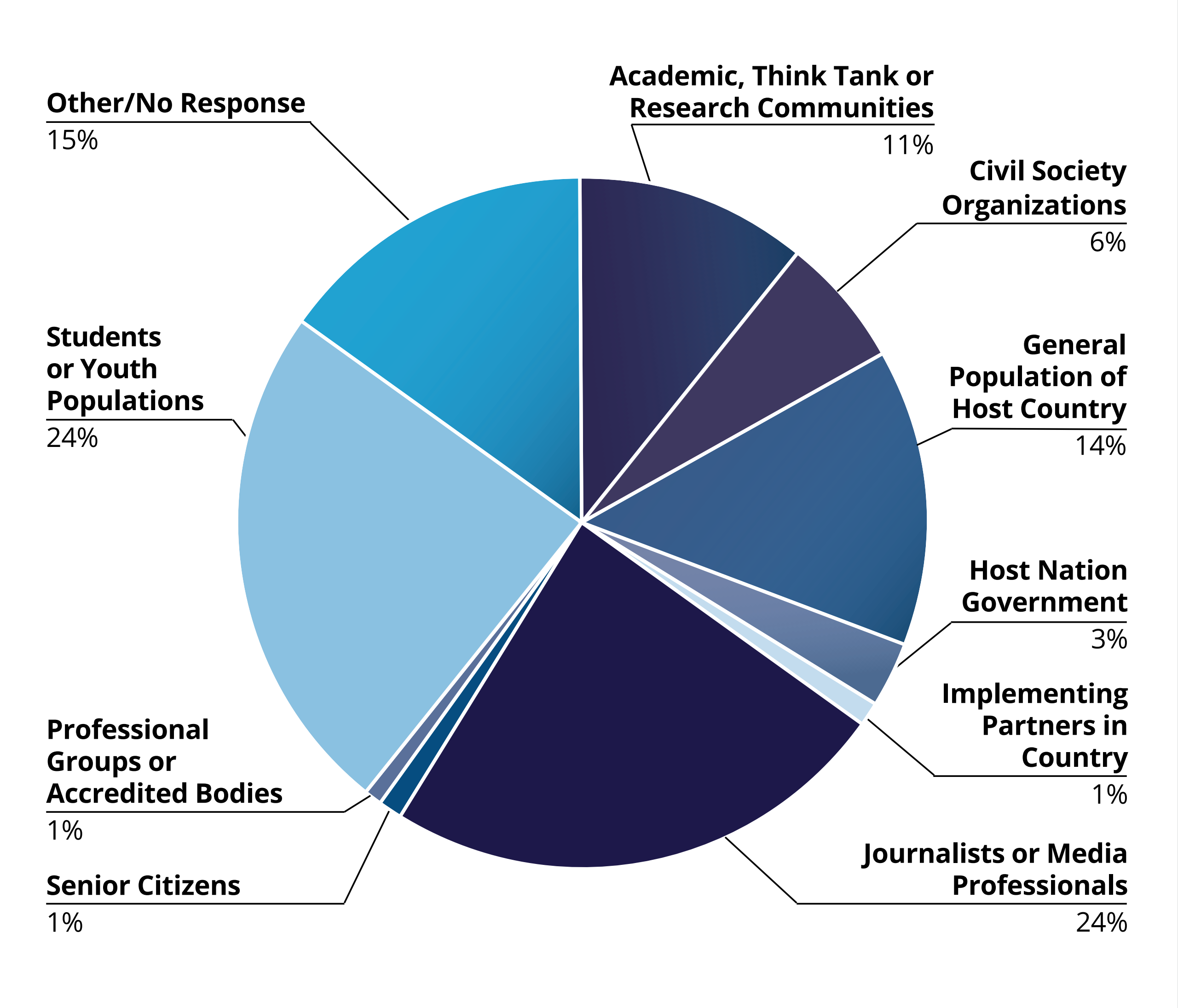
Post-Reported CSD Programs Sorted by Primary Objective



Graph J: *Post-Reported CSD Programs Sorted by Target Audience*

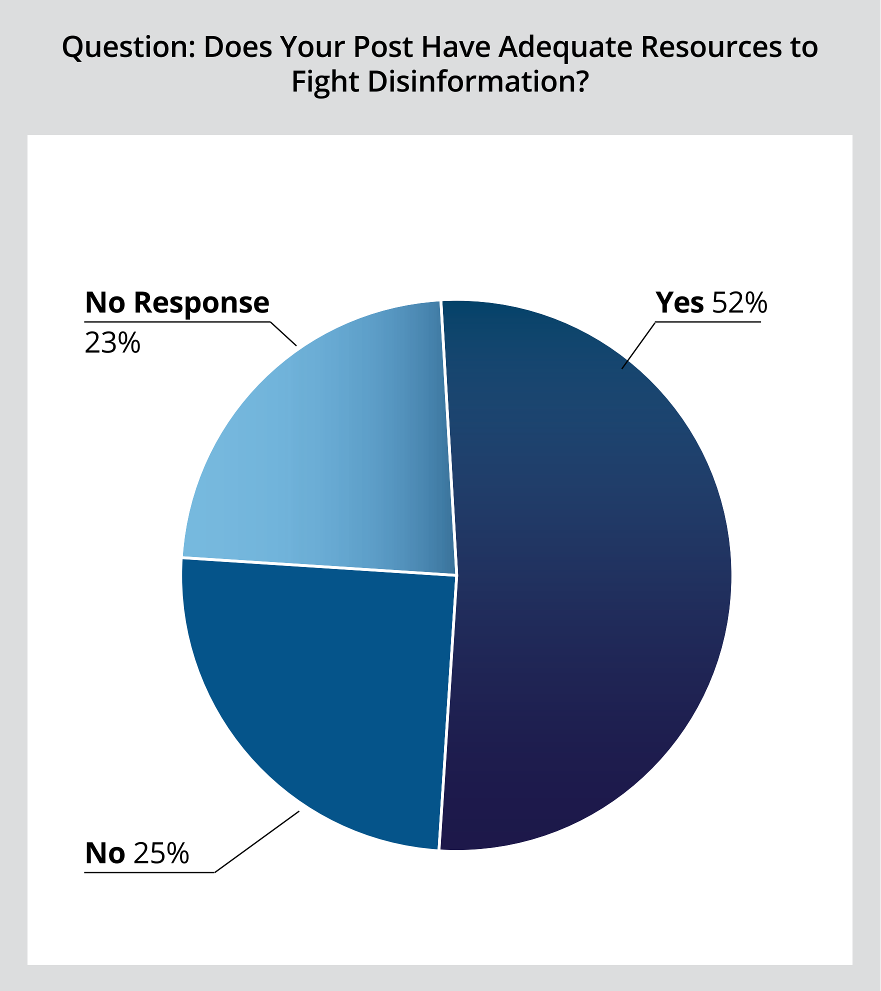
The pie chart featured in Graph J indicates a clear preference for CSD programming that builds resilience and capacity building through training and education—with a strong successor generation focus. Posts reported that 59 percent of their programs were intended for journalists (24 percent), youth or students (24 percent), or academics (11 percent). Other key audiences include civil society organizations, professional organizations, and implementing partners who serve to further promote and sustain counter disinformation efforts.

Post-Reported CSD Programs Sorted by Target Audience



Graph K: *Does Your Post Have Adequate Resources to Fight Disinformation?*

As the Graph K pie chart shows, a little more than half of the respondent posts indicated they had adequate funding for CSD activities, while 25 percent indicated that they did not. Rather than concluding that half of all posts considered themselves adequately prepared to meet the state-sponsored disinformation threat, however, we believe this should be interpreted to contextualize the previous response categories. Specifically, since posts self-selected to respond, this likely indicates that the responses above most aptly apply to posts that are *already* engaged in what they believe is an effective strategy to counter state-backed disinformation. Conversely, a significant proportion of posts that did not respond likely either did not have CSD programming to report, and/or did not meet their own assessment that they were adequately countering the state-sponsored disinformation threat.



Diagnostic Summation

It is clear that from 2016 to 2019 there was a significant increase in focus on efforts to counter state-sponsored disinformation activities across the USG PD community. While at first the CSD response was relatively uneven and disjointed, by 2019 the sheer amount of focused attention had, by some measures, even matched the post-9/11 focus on countering violent extremism. This led to a significant restructuring of the largest USG PD entities in a very short period of time. Meanwhile, the Department of State and USAGM introduced critical new technologies and skills to the PD mix to better meet the reemergent state-sponsored disinformation threat.

> Experts…agreed that the disinformation threat cannot be countered through educational programs alone; the threat is increasingly digital in nature, and accordingly, the PD community should prioritize mastery of the digital domain.

In each of the datasets the ACPD analyzed (raw cable traffic, strategic planning documents, interviews, and a data call sent to all posts), EUR represented an outsized proportion of overall CSD activity.[25] Furthermore, these activities fell into a familiar, Cold War-inspired programmatic framework, including long-term investments in education-related activities, sustained focus on host government capacity building, the development of independent journalism networks, and the promotion of resilience within key audiences. Deterrence and messaging received far less attention, at least initially, in terms of CSD programming.

Virtually everyone the ACPD interviewed agreed that state-sponsored disinformation activities were not exclusively a European issue, but instead represented a fast growing global phenomenon. In 2019, a study by the Oxford Internet Institute found evidence of state-backed "social media manipulation campaigns" in 70 countries – a significant increase over an earlier study just two years prior that found just 28.[26] Additionally, most experts and several former senior PD officials interviewed for this study agreed that the disinformation threat cannot be countered through educational programs alone; the threat is increasingly digital in nature, and accordingly, the PD community should prioritize mastery of the digital domain. While all believed that educational programs were core to PD programming and critical to "creating a foundation for democracy and critical thinking," they also warned that retrofitting the goals of existing educational programs to counter-disinformation priorities would not be a sufficient response because they do not actively impact the information environment, which is constantly under siege by advanced state-backed actors.

A proactive digital presence alone cannot overcome the corrosive effects of deliberate disinformation campaigns. Narrative control is required.

Counter disinformation expert Clint Watts compares the problem of cyber threats to today's disinformation challenges, noting a need for more and better digital tools to stay ahead of the threat:

> *A decade ago, there was a similar problem in tackling the toughest cyber threats. Advanced Persistent Threat (APT) actors emerged, conducting sophisticated, well-resourced hacking efforts that access networks and remain undetected inside them for prolonged periods… Western companies and governments have undertaken approaches for understanding and combatting APTs that can be instructive for social media companies as they defend against the greatest challenge in their history. Tackling the most advanced threats to platforms requires a new, sustained approach to thwart nefarious manipulation. This intelligence-driven approach begins with an improved understanding of the threat actors and the methods they deploy via social media.*[27]

This is particularly true in countering "grey" disinformation or propaganda, which, unlike outright fabrications, consists of distortions of real events that can frame attitudes and opinions. This digital information manipulation might not make it into a senior USG official's briefing book on a regular basis, but it is important because it has the potential to slowly and quietly undermine long-term USG policy initiatives.

Ultimately, a proactive digital presence alone cannot overcome the corrosive effects of deliberate disinformation campaigns. Narrative control is required. As a former senior PD official at the State Department noted: "One of the truisms of modern media is that the person whose story wins is usually the person who frames the narrative, and we need to do a better job of framing that narrative."[28] Effective narrative framing in a hostile information environment begins with a good understanding of prevailing contexts and actors. The next section of this report assesses both in a review of field-level CSD programs and impacts.

PART III: CSD IN THE FIELD: PROGRAM IMPLEMENTATION AND IMPACTS

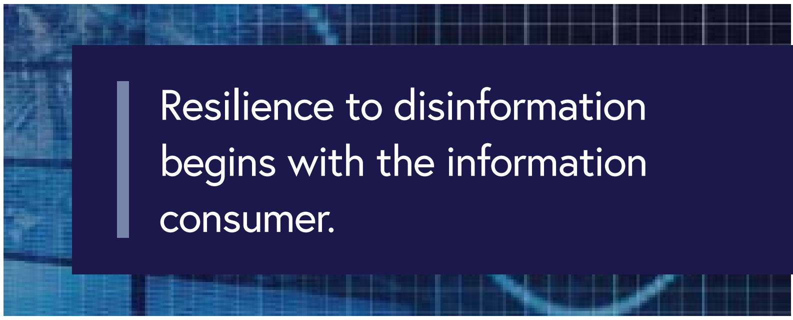
In order to assess CSD program implementation and impacts in the field, the ACPD conducted a series of research visits to five European countries—Iceland, Finland, Latvia, Hungary, and Georgia—in Fall/Winter 2019. This section of the report provides an overview of current Washington-based resources for field programs before turning to an examination of CSD program implementation at the USG post level. It then offers host country perspectives on current and future efforts to combat malign influence threats.

Current Washington-Based Resources for Field Programs

Effective measures to counter disinformation in the field begin with the effort to identify, classify, research, and monitor current malign influence strategies. This includes research initiatives to identify and track malign influence trends, themes, and behaviors, as well as to obtain accurate analyses of target audiences' interests and vulnerabilities. The GEC plays a critical role in the effort to map the actual digital consumption habits of target populations and to provide a clear picture of disinformation transmission patterns—and how to anticipate them.

Public diplomacy CSD speaker, specialist, and short-term exchanges build resilience by supporting independent media. Programs aim to improve the digital communications capacities of credible messengers, including government officials, journalists, educators, and civil society actors. Targeted training and short-term programs for journalists on topics such as investigative journalism and reliable content generation strengthen independent media outlets. A number of PD initiatives promote the development of open source information resources and analysis through training programs as well as the development of collaborative information exchange networks.

PD programs have also enabled independent media platforms to play an active role in deterrence, especially accessing and disseminating news and information from a broad range of sources to mitigate disinformation effects. For example, USAGM broadcast and social media platforms provide access to objective, language appropriate international, regional, and domestic news and news for use in domestic/regional contexts. They also promote information flows into restrictive environments and marginalized communities with minimal access to credible media outlets.



Resilience to disinformation begins with the information consumer.

Resilience to disinformation begins with the information consumer. It is essential to teach vulnerable audiences to identify false stories and hate speech, discern fact from opinion, and crosscheck facts and sources. Media literacy training programs for journalists, educators, and civil society actors inoculate information consumers against the emotional, hyper irrational appeal of coercive or potentially destabilizing narratives. PD programs have also supported the creation of viable, professionally managed online fact checking organizations to provide accurate information, counter falsehoods, debunk myths, and expose disinformation tactics.

Sustained investments in soft power initiatives create the conditions for resilience. Specifically, a wide range of cultural and educational exchange programs—the proverbial "last three feet" of public diplomacy engagement—builds audience capacity to resist the spread of disinformation effects. Art, music, dance, theater, and film programming provide much needed context and depth to an overloaded media space in which an abundance of information results in a scarcity of attention and understanding. Short-term professional exchanges enable information sharing and collaboration, while longer term academic exchange programs build skills and provide a deeper understanding of political, social, and economic contexts. Finally, cultural and educational exchange programs support greater receptivity to USG policy-oriented messaging.

Post Perspectives: Implementation at the Field Level

We wanted to understand how these Washington-designed and funded programs play out at the field level. We were particularly interested in challenges to effective implementation raised during the 2019 global public diplomacy conference. Several public diplomacy officers currently working at overseas missions, including those who described themselves as being on the "front lines" of CSD campaigns, noted that GPA and GEC were not always able to support their efforts. They expressed concern that the new PD bureaus and offices were designed to respond to top-down messaging priorities rather than supporting field-based initiatives. This focus on Washington could create a disconnect in CSD program coordination, they warned, because it might come at the expense of post specific needs with respect to CSD program content as well as resources.

> The success of CSD programs depended largely on post's understanding of host country vulnerabilities to disinformation as well as public and private sector attitudes toward and experiences of malign influence effects.

These observations were generally borne out during our field visits. Although we did not detect evidence of an outright strategic disconnect between Washington priorities and post initiatives, we found that CSD program resources required extensive tailoring to meet host country needs and capabilities. The success of CSD programs depended largely on post's understanding of host country vulnerabilities to disinformation as well as public and private sector attitudes toward and experiences of malign influence effects. This is especially important when, for example, the host country government does not consider disinformation to be an existential threat. We also found evidence of CSD program saturation, e.g. too many resources directed at a relatively narrow range of local CSD challenges. This can result in a certain level of program fatigue among key audiences, and raises questions about effective resource distribution.

We also found evidence of CSD program saturation, e.g. too many resources directed at a relatively narrow range of local CSD challenges. This can result in a certain level of program fatigue among key audiences, and raises questions about effective resource distribution.

The following country-specific CSD program descriptions illustrate the extent to which post CSD programming has been successfully adapted to the local context:

Iceland

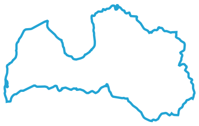
To address growing concerns about disinformation effects in Iceland, PAS Reykjavik has focused its efforts on media literacy training with a view to building fact checking and data analysis into the national public school curricula. PAS Reykjavik has also stepped up efforts to support training in investigative reporting for local journalists to improve the credibility of media institutions among domestic audiences. This includes an effort to provide access to advanced audience research and assessment tools as a basis for improved analysis of media content and sources. Finally, a PAS Reykjavik-sponsored grant offered a speaker program on the intersection of technology and disinformation as well as support for a University of Iceland administered conference on hybrid threats co-sponsored by the European Union and the United Kingdom.

Finland

To mitigate the potential for malign influencer interference, PAS Helsinki managed a $500,000 GEC-funded grant to the European Hybrid Center of Excellence to conduct electoral interference and open source intelligence training. U.S. speaker Rand Waltzman, the Rand Corporation's Deputy Chief Technology Officer, participated in a Hybrid COE/EU Commission minister-level panel on disinformation during Finland's EU presidency. Fulbright and other U.S. speakers focused on topics such as "Truth Matters: Strategies for Combating Manipulated Realities" and "Making Democracies Resilient to Modern Threats." Finally, a PAS/GEC-funded regional reporting tour for 15 journalists from France, Belgium, and Germany brought journalists together with disinformation and hybrid influence experts from civil society, the media, academia, and the Finnish government, including from the Ministry of Defense, the Prime Minister's Office, and the Ministry of Foreign Affairs.

With support from member states, to include the United States, the European Center of Excellence for Countering Hybrid Threats has developed programming to support NATO and EU allies to identify and combat disinformation and malign influence campaigns ahead of European elections. In addition to the traditional focus on citizen education and outreach and electoral process management, Communications Center of Excellence (COE) programs address resilience building measures such as broad interagency cooperation and information sharing. COE experts report that typical government shortfalls include the failure to communicate effectively about electoral processes and outcomes with local populations. Lack of situational awareness about the potential for external influencers to use social media platforms to interfere with domestic electoral processes is a persistent problem. Finally, the absence of cooperative relationships between government and social media platforms remains a critical vulnerability.

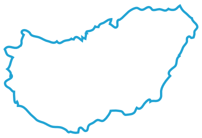
Latvia



PAS Riga CSD programming focuses on developing public awareness of disinformation tools and objectives through a combination of speaker, training, and exchange programs targeting the spread of disinformation, media literacy, and investigative journalism. Speaker programs have addressed building media literacy skills into public school curricula and providing hands on media literacy skills development for teachers. Various regional professional journalist programs focus on issues such as advanced research and fact-checking techniques as well as investigative reporting in vulnerable regions. Targeted short-term professional exchange programs have sent Latvian journalists on disinformation-related reporting tours, with a focus on developments in Ukraine and NATO exercises in the region.

Youth-focused CSD programming builds on the presence of Fulbright English Teaching Assistants and English Language Fellows in higher education institutions, as well as targeted embassy outreach to students in Russian language schools. Youth entrepreneurship programs also reinforce basic media literacy skills. Grants to local media NGOs have supported collaborative news and information verification initiatives. Finally, PAS collaboration with the NATO Strategic Communications Center of Excellence in Riga has facilitated meetings with government leaders, media, and civil society working on countering disinformation effects.

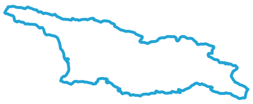
Hungary



PAS Budapest has partnered with local academic institutions, thinks tanks, and NGOs to promote media literacy among journalists, educators, civil society actors, university students, and targeted rural populations. Approaches ranged from building audience capacity to identifying fake news and propaganda to more sophisticated research and analytical skills building. Speaker programs addressed propaganda threats posed by social media technology and provided exposure to products and services to protect against advanced cyber threats.

Targeted exchange programs have sent Hungarian media and academic sector representatives to programs on media responsibility as well as advanced journalism and media literacy training. An investigative journalism initiative trained young reporters to produce stories exposing evidence of corruption in the public sector. Several American Corner events supported CSD initiatives, such as a three-day course in one regional capital that provided students with hands on strategies for identifying, filtering, and analyzing information online. Another regional event helped teenagers to identify fake news and advertising, develop data protection skills, and create effective news content.

Georgia



A large percentage of PAS Tbilisi program funds focuses on countering disinformation effects, much of it centered on media training and capacity building. In cooperation with PAS Baku and PAS Yerevan, PAS Tbilisi hosts graduate level journalism training, to include professionalization and investigative reporting. Direct grants to local media outlets enable the production of short infotainment programs that communicate the importance of sustained economic and security ties to the United States and the West. PAS Tbilisi also supports media literacy training programs that focus on high school and university students as well as journalists.

Other PAS-sponsored programs increase the capacity of local influencers such as teachers, journalists, and civil society actors to promote viable counter narratives to extremism. A large PAS Tbilisi grant facilitated the development of a Strategic Coordination Unit within the Georgian government to foster coordination and standardization of official strategic communication efforts. Finally, small scholarship programs in 29 vulnerable minority communities offer English language classes as well as short courses on civics and technology topics.

Host Country Perspectives: Building Resilience, Improving Deterrence

In addition to learning more about post implementation of CSD initiatives, we wanted a better understanding of the program environment from the host country perspective. Our conversations with government officials, journalists, academics, and media-focused NGOs revealed important similarities and differences in each country's experience of disinformation effects, and provided useful context for assessments of CSD program effectiveness.

Not surprisingly, a country's historical, geographical, and cultural relationships play a key role in its relative vulnerability to disinformation effects. For example, the former Soviet satellite states that now share a border with Russia have historically been at the mercy of Russian military and economic ambitions, as well as religious and cultural dominance. With the collapse of the USSR, the newly independent states, also known as the "near abroad," posed an even more existential threat to Russia's security and prosperity, especially as these countries moved to greater integration with transatlantic security and economic institutions.

> Our interlocutors agreed that the power of disinformation lies in the ability to exploit prevailing political, economic, and social vulnerabilities.

Our interlocutors agreed that the power of disinformation lies in the ability to exploit prevailing political, economic, and social vulnerabilities. In general, we found that these vulnerabilities fall into four broad categories: historical, geographic, and cultural legacies; current governance practices and adherence to the rule of law; economic conditions and the effectiveness of social security guarantees; and the extent to which information is broadly accessible and free, and open and independent media institutions prevail. Taken together, assessments of these four elements can serve as a fairly reliable indicator of disinformation impacts in a particular country. They also provide a framework for longer term resilience-building initiatives.

Kremlin-produced disinformation narratives attempted to discredit these efforts, employing both threat and suasion. The threat of sustained or renewed conflict with Russia lends enormous power to disinformation narratives that invoke Russia's might while denigrating a state's capacity to guarantee national security and prosperity. At the same time, Russia's morally superior, pan-Slavic narratives lay claim to culturally embedded shared values.

Inevitably, these narratives play to deep-seated fears about the loss of traditional social practices and beliefs as a consequence of integration into Western security and economic institutions. While these effects are less prevalent in the Baltic states, such as Latvia, which have achieved full NATO and EU membership, aspirant countries such as Georgia are particularly susceptible to stories about the moral and spiritual corruption of the West.

The presence of ethnic minority populations in the countries of the near abroad offers additional opportunities for narrative exploitation on the basis of linguistic isolation, economic dislocation, and political disenfranchisement. It is easy for disinformation narratives to make the case that these groups have been abandoned by the state to offer, instead, the assurance of support based on a shared common language—Russian—and promises of sustained economic and security support.

> While the countries of Russia’s near abroad remain uniquely vulnerable to Russian disinformation narratives, Central European countries are also at risk. Disinformation effects are propagated through domestic political exploitation of perceived failures to protect security and economic interests.

While the countries of Russia’s near abroad remain uniquely vulnerable to Russian disinformation narratives, Central European countries are also at risk. Disinformation effects are propagated through domestic political exploitation of perceived failures to protect security and economic interests. For example, in Hungary, the painful legacy of Soviet occupation and repression was an important driver for its initially strong embrace of democratic principles and successful integration into NATO and EU institutions. More recently, Hungary’s increasingly authoritarian government has produced an anti-Western, anti-democratic narrative that blames the West for Hungary’s security and economic vulnerabilities. Elements of this rhetoric closely resemble those found in Kremlin-based denunciations of Western aggression and immorality.

Finland and Iceland present interesting variants on the domestic exploitation of disinformation narratives. No stranger to Russian invasion, most recently during WWII, Finland built a strong postwar democracy focused on strength through cohesion and collective security. Nevertheless, the memory of Soviet occupation and the need to remain vigilant has the potential to be exploited by fringe groups on either end of the political spectrum. As an island nation far removed from the threat of Russian occupation, Iceland has had little to fear from Russia. However, in the absence of a national military, conflicted public attitudes prevail about Iceland’s reliance on the United States and NATO for security. This in turn provides opportunities for fringe elements of the opposition to produce narratives about, for example, the government’s willingness to compromise national sovereignty.

With respect to internal governance, vulnerability to disinformation effects appears to be greatest in countries that have relatively recently transitioned into democracies (what some experts have identified as the “young democracy” phenomenon). Resilience requires relative social cohesion, a general consensus about national identity, trust in the political process, and confidence in the capacity of government (popular trust) to meet citizen needs—all more or less present in established democracies. In countries like Georgia, by contrast, popular frustration with the slow pace of political, economic, and social reforms, and perceptions of government corruption and/or incompetence create receptivity to disinformation narratives that highlight state failure to protect citizens’ economic and security interests.

> With respect to internal governance, vulnerability to disinformation effects appears to be greatest in countries that have relatively recently transitioned into democracies.

Failures, perceived and actual, in a country’s social security network also create fertile ground for malign influence effects. In Georgia, for example, recent polls indicate that people are most worried about job security, rising costs, pensions, and access to health care. Disinformation narratives exploit these concerns, attributing them to a failure in national leadership and the unreliability of Western-inspired democratic institution building. By contrast, Finland’s “depoliticization of equality,” generous social welfare benefits, and regulation of the labor economy creates a relative immunity to politically motivated disinformation narratives.

Finally, deeply polarized societies with low trust in media institutions and a history of government sanctioned controls on information access and outreach are especially susceptible to disinformation effects. In newly independent states such as Georgia, the early proliferation of unregulated news media outlets, partisan control over a significant portion of the media landscape, and public mistrust of official media sources created the ideal conditions for the dominance of Russian-driven disinformation narratives. By contrast, in Hungary, where the government has near complete control over the national media space, the disinformation threat is largely internal, emerging primarily from ruling party interests.

> Failures, perceived and actual, in a country's social security network also create fertile ground for malign influence effects.

> Deeply polarized societies with low trust in media institutions and a history of government sanctioned controls on information access and outreach are especially susceptible to disinformation effects…Low trust in governance also exacerbates vulnerability to destabilizing influencers, both external and internal.

The following country-specific assessments of disinformation effects offer specific examples of vulnerabilities to disinformation effects as well as measures necessary to address them.

Iceland

Compared to the other countries in this report, Iceland represents something of an outlier in its experience of disinformation effects. Indeed, according to Iceland's Media Commission, Russian, and to a lesser degree Chinese disinformation efforts, have only recently been acknowledged as a national security threat within the Icelandic government. This may have to do with what several officials described as Iceland's "island mentality," which fosters a strong sense of national identity and social cohesion.

But, while this island mentality may shield Iceland's citizens from external efforts to inform and influence, it also contributes to what one official described as a kind of "geopolitical illiteracy" or lack of awareness of and appreciation for Iceland's external political, economic, and security commitments. This in turn creates a certain vulnerability to disaffected narratives about the government's failure to place its citizens' needs above foreign policy imperatives.

This is particularly true with respect to the lack of public trust in the United States and NATO. According to Ministry of Foreign Affairs officials, the Russian disinformation narratives that have penetrated Iceland's media space echo anti-George Soros themes, critiques of the international sanctions regime, the U.S. and NATO-driven "militarization of the Arctic," and the international community's responsibility for Syria's humanitarian crisis inflicted by the U.S./NATO. While these narratives are concentrated in the 10-15 percent of the population associated with far-right political parties, their presence nevertheless represents a threat to Iceland government officials' attempts to make the case for greater involvement in international political and economic systems and structures.

Increasingly, low trust in governance also exacerbates vulnerability to destabilizing influencers, both external and internal. For example, the 2008 financial crisis is seen by many as the Icelandic government's failure to regulate the financial sector and protect citizens from bankruptcy. Iceland ranks high (94/100) on Freedom House's Free Media index, and state media channels enjoy a certain level of credibility. Nevertheless, Icelandic officials are concerned about a declining trust in commercial media, which is perceived as "corrupt and gossip laden," with editorial policies "driven by commercial interests." Icelandic officials also note a deterioration in the relationship between Iceland's political figures and domestic media outlets, a gap easily exploited by domestically-driven disinformation narratives.

Government officials and academic and media experts see a need to broaden the Icelandic public's understanding of key geopolitical issues such as energy distribution and climate change. They also note that the politicization of issues such as Iceland's role in NATO and its "security dependence" might be mitigated by a more consciously transparent public dialogue about Iceland's security needs. Finally, they seek measures to rebuild credibility among commercial media outlets in order to assure greater diversity in the Icelandic media space.

Finland

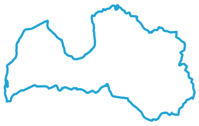
The Finnish government claims a relatively low level of vulnerability to disinformation effects owing to its "Comprehensive Security Approach," which one official described as a broad, multisectoral consensus on national security priorities. A national identity built on shared values, a generally non-polarized media landscape, and a high level of media literacy also provides a certain immunity to disinformation narratives that might otherwise exploit perceived social and political inequities.

Nevertheless, Finland is taking steps to raise public awareness of propaganda to prevent the erosion of popular trust in government. These measures include

> A national identity built on shared values, a generally non-polarized media landscape, and a high level of media literacy also provides a certain immunity to disinformation narratives that might otherwise exploit perceived social and political inequities.

a national level campaign to expose disinformation narratives and provide countervailing, fact-based rebuttals. The Finnish government also cites efforts to analyze disinformation sourcing and methods—and to make research results broadly available to the public, including journalists and educators. Finally, Finnish government officials are working closely with private sector partners to address the threats posed by Deep Fakes and other Artificial Intelligence tools to national security and prosperity.

Latvia



Latvia, like its neighbors Estonia and Lithuania, has experienced several hundred years of conflict with Russia, to include territorial aggression and occupation. Situated on the border with Russia, Latvia looks to its NATO and EU memberships as its best defense against Russian Federation attempts to destabilize the country, both on the ground and in the information space.

According to Ministry of Foreign Affairs officials responsible for leading the effort to counter disinformation effects, there are several factors that work in Latvia's favor. First, thanks to Latvia's geographic proximity and long history with Russia, there is a high level of domestic awareness of Russian disinformation themes and strategies. Moreover, the Latvian government does not view disinformation in isolation but rather addresses it as part of a broader national security challenge. This permits the use of multiple resources and a broad multi-sector approach to the problem.

Finally, the Latvian government understands that effective counter disinformation measures need to focus on building domestic resilience to its most potent effects. As one official noted, Russian behaviors—especially the reliance on destabilizing influence measures—are not going to change. According to local experts, what can (and must) change is public understanding of and ultimately confidence in Latvia's political and media institutions. This would require the Latvian government to focus on greater information sharing, especially with respect to policies that may seem to disadvantage or create short-term pain for domestic audiences. The conditions required for resilience to disinformation also include the fostering of a free and open media environment.

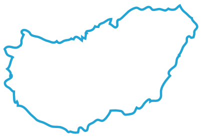
> The Latvian government does not view disinformation in isolation but rather addresses it as part of a broader national security challenge. This permits the use of multiple resources and a broad multi-sector approach to the problem.

NATO Strategic Communications Centre of Excellence (Riga, Latvia)

As part of its broad based, multisectoral approach to countering disinformation effects, the Riga-based NATO Strategic Communications Centre of Excellence COE has prioritized monitoring and assessment of the information distribution channels used by social media platforms. COE officials see the need to align the "Silicon Valley business model" of information dissemination and consumption with the promotion of democratic values and the protection of individual rights and liberties. They also note the need for a broad-based dialogue about the nature and quality of social media sector governance that addresses issues such as individual privacy vs. collective security and transparency vs. operational security.

NATO COE experts recognize that social media platforms have a dual responsibility to their users to guarantee their privacy as well as their security. Additionally, they acknowledge the need to avoid content regulation and data privacy violations. At the same time, they feel strongly that social media companies must share public interest data about movements or trends that may have serious implications for national security. They also note the need for greater transparency about consumer information data collection and usage practices as well as algorithm development, analytics, and applications.

Hungary



Hungary's experience of disinformation effects is distinguished by its government's increasingly authoritarian behavior and apparent rejection of the liberal democratic narrative. Some experts see Prime Minister Orban's surprisingly forceful anti-Western rhetoric as a partial reflection of the Russian Federation's core disinformation narrative about the corrupting influence of Euro-Atlantic institutions. Others view the Hungarian government's strident illiberalism as a legacy of its transition to independence in 1989 – the failure of the then new leadership to embed liberal democratic principles into its political philosophy.

In any case, Orban and his associates have perfected a policy narrative that, like Russian disinformation narratives, builds on a basic mistrust of democracy and democratic principles. Orban capitalizes on this fear to foster a collective sense of insecurity in Hungary's ability to project power—and to justify illiberal measures such as legislated restrictions on judiciary and parliamentary powers and the slow asphyxiation of Hungary's independent media. Indeed, Orban's return to power in 2010 was marked by creation of a party-driven media consortium along with a legislative approach to limiting/controlling access to information.

Thanks at least in part to its highly centralized and near monopolistic control of the press, the Hungarian government, rather than outside actors, appears to be the primary source of disinformation. Though perhaps inspired in part by Russian

> Thanks at least in part to its highly centralized and near monopolistic control of the press, the Hungarian government, rather than outside actors, appears to be the primary source of disinformation.

sources, Hungary's home-grown narratives emerge largely from the ruling party, to a lesser degree from the opposition, and occasionally from fringe elements on the far right and left of the political spectrum. Some experts claim that pro-government media institutions actually function as "disinformation factories" that essentially do the work of Russian disinformation outlets such as RT and Sputnik. "Fake news" stories, adapted to justify policy actions, have become part of the government's political narrative. Finally, the uniqueness of the Hungarian language also intensifies disinformation effects, which do not seem to be mitigated by unrestricted access to social media platforms and international news and information sources.

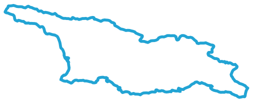
Experts warn that the government's ongoing restructuring of the media landscape supports ruling party, rather than national, interests—especially in economically and socially vulnerable rural areas. This has created a potentially destabilizing information gap between Budapest and the regions. The centralization of information dissemination also contributes to a growing sense of "apathy" among university students, especially in rural regions, who, according to experts, are more interested in preserving the status quo and finding jobs than engaging in political activism.

A few independent media experts argue, with some asperity, that in general the Hungarian majority doesn't care about diminishing media freedoms because "it doesn't see that it has been deprived of information." These experts go on to make an interesting distinction between the freedom of speech, which exists in Hungary, and the freedom to access information, which, in Hungary's centralized media environment, is at risk. Said one media representative: "Journalists are free to ask the hard questions. They just don't get answers." Media experts also point to the "ghettoization of media in Hungary," which is resource deprived thanks to government control of access to the advertising sector.

Despite these challenges, local observers concur that the potential exists to counter disinformation effects in Hungary. First, they recommend that a concerted effort be made to fill knowledge gaps in vulnerable rural areas, where information content is largely national in focus. Arguing that there is a genuine desire for local and regional as well as international news and information, several experts recommend the creation of a broad-based coalition of independent online media sources to provide content targeted at local needs and interests. They also suggest the creation of a network of regional correspondents reporting on regional news.

With respect to the national media scene, Hungarian media and civil society experts call for the inclusion of local and regional issues in the now largely centralized discourse about political, economic, and social issues. They also advocate for more balanced popular understanding of and engagement in global issues with domestic implications, such as climate change and immigration. Finally, experts note the need for more diverse content generation, especially with respect to the West, which is largely framed in negative, anti-imperialist or capitalist terms. Civil society organizations must be empowered to produce alternative discourse elements and expand content.

Georgia



As a former Soviet satellite state seeking lasting relationships with Euro-Atlantic institutions, Georgia has been subjected to long-term, punitive Russia disinformation campaigns since its independence in 1991. Georgia's 2003 Rose Revolution, which resulted in a peaceful transition of power, was heralded as a "new wave of democratization" for the region. But Russia's 2008 invasion of Georgia, and subsequent occupation of South Ossetia and Abkhazia, highlighted the fragility of Georgia's status as an independent, sovereign state. Russia's campaign to bring Georgia back into its sphere of influence has forced Georgia to confront existential questions about national identity, values, and prevailing models of governance.

Despite these challenges, Georgia has made some significant progress in the effort to counter Russian disinformation effects thanks to the support of the international community. NATO, the EU, the United States, the United Kingdom, and many other countries have contributed to this effort in the form of media literacy and journalism training programs, grants to support the development of independent fact checking organizations, support for the development of a viable strategic communications infrastructure within the national government, targeted information and outreach campaigns in support of EU and NATO integration, and so on.

Nevertheless, the information environment remains fragile. Local experts report that disinformation in the form of fake or manipulative news stories has become the "new normal" in the national media space. They also note that disinformation is increasingly domestic in origin, often amplifying extremist (far left and right) attitudes. Public and private sector representatives underscore the increasing polarization of Georgia's commercial media space, especially domestic television stations. Reports indicate that trolling, particularly by government-affiliated bots and users, has intensified, most notably during the runups to parliamentary and presidential elections.

Experts also link the intensification of disinformation effects to the slow, and necessarily demanding, pace of EU and NATO integration. Both Russian and domestic disinformation narratives ably exploit the popular knowledge gap about the EU integration and NATO accession processes. They also reflect precise awareness of vulnerabilities, highlighting, for example, the short-term economic and social risks and costs of the reforms necessary to meet EU benchmarks. These narratives focus on the relative ease of doing business with Russia, to include higher short-term profit margins, fewer tariffs, and the absence of export regulations for locally produced agricultural products.

With respect to NATO, disinformation messaging in Georgia is double edged. On the one hand, narratives suggest that the slow pace of NATO accession means that the West is abandoning Georgia.

> Experts also link the intensification of disinformation effects to the slow, and necessarily demanding, pace of EU and NATO integration. Both Russian and domestic disinformation narratives ably exploit the popular knowledge gap about the EU integration and NATO accession processes.

Russia, on the other hand, is "winning in the region" because it appears to be operating from a position of strength. In fact, Russia's occupation of 20 percent of Georgia's territory, along with periodic escalation of hostilities along the disputed borders, effectively holds Georgia in thrall. Disinformation narratives also exploit NATO's reluctance to get drawn into a conflict with Russia over Georgia's sovereignty.

A range of social and cultural factors contribute to the enduring power of disinformation narratives in Georgia. Georgia's Orthodox clergy remain divided on the question of political and spiritual association with Russia. In fact, some experts believe that the upcoming succession battle for the new Georgian Patriarch may fall along Russian vs. EU lines. Armenian and Azeri minority communities, particularly those along the border of Armenia and Azerbaijan, suffer from linguistic isolation, a vulnerability which promotes reliance on Russian language sources. Reports also indicate the persistent presence of pro-jihadist elements within the Georgian far right, primarily on the basis of a rejection of so-called Western values. Finally, small but persistent elements of xenophobia, homophobia, and religious conservatism remain powerful disinformation drivers.

To address Georgia's vulnerability to disinformation effects, government officials, media, and civil society experts see the need for broad-based cross sector coordination. So far, Georgian government efforts to counter disinformation remain relatively uncoordinated and reactive, compromised by, on the one hand, significant support for Russia on economic grounds (Georgia's rural population depends on exports to Russia) and, on the other hand, by the all too real threat of Russian military aggression. The current absence of coordination on local, regional, and national lines among military, law enforcement, and government ministries/agencies leaves Georgia vulnerable to asymmetric information attacks.

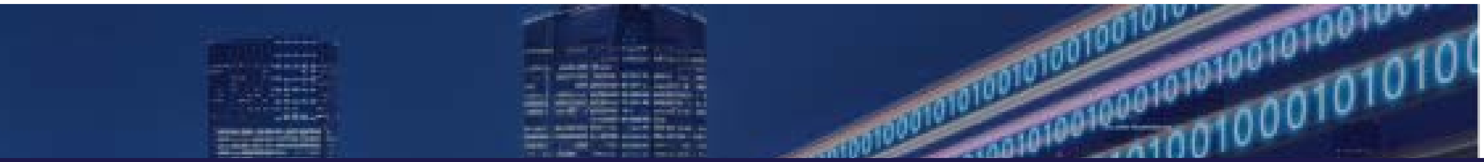
Government, media, and civil society actors agree on the need for better disinformation impact assessments to better understand the scope and evolution of the threat in Georgia. They also call for improved program monitoring and evaluation resources for existing CSD programs. This includes the development of language-specific software/analytic tools to monitor and assess disinformation streams, enhancement of audience research capacities, and enhanced mapping of target audience vulnerabilities. Finally, experts need to foster proactive cooperation rather than divisive competition and duplication of effort among the NGOs working on countering disinformation effects.

CONCLUSION

These country-level assessments confirm that effective counter disinformation activities require a mix of broad resilience building strategies and actor-specific deterrence tactics. The threat of disinformation emerges from its potential to exploit prevailing political, economic, and social deficits—both perceived and actual. Therefore, building resilience to disinformation effects must begin with a realistic identification of these vulnerabilities, as well as the national capacity to address them. Once these vulnerabilities have been identified, targeted deterrence measures which push back on specific elements of disinformation narratives come into play. As this report attests, much good work has already been done through PD programs that build resilience to disinformation effects while improving measures of deterrence through short-term training and content development programs, as well as long-term civil society and democratic institution building initiatives.

Nevertheless, more needs to be done to address a continuously evolving operational environment, from the emergence of new tools and technologies to shifts in geopolitical relationships. One senior counter-disinformation official at the center of the changes described in this report told the ACPD that "we have witnessed…the first structural innovations of a new post-Cold War internet era, but they won't be the last." The official cautioned, "Our ability to move forward will come down to how we are able to change and adapt to the emerging order. Government institutions don't change by themselves."[29]

Indeed, what distinguishes the Cold War experience of disinformation effects from



> We have witnessed…the first structural innovations of a new post-Cold War internet era, but they won't be the last. Our ability to move forward will come down to how we are able to change and adapt to the emerging order.

> We have always been—and always will be—at war over influence in the global information space.

the current threat environment is the rapid and multifaceted transformation of the global information infrastructure. This report indicates that current CSD PD programs and resources must be attuned and continuously responsive to the digitization of the information space. At the same time, however, there needs to be consensus about strategic priorities, as well as a more realistic set of expectations about influence management in the global arena.

The ACPD's recommendations focus on improvements to the PD toolkit to address these evolving threats. The establishment of a shared lexicon of disinformation will facilitate overall CSD program coordination and resource distribution. Greater investment in digital capabilities, and improved capability to fund short-term, experimental initiatives will improve program flexibility and responsiveness. Personnel and infrastructure upgrades such as the creation of a job series for mid-career CSD specialists and the reconfiguration of PD sections at post will improve field-level engagement with the digital information space. Finally, long-term program effectiveness requires the ability to evaluate and monitor CSD programs at scale and assess impact. All of these recommendations balance longer-term resilience and capacity building measures with shorter time horizon initiatives such as deterrence and messaging, which are no less important in a complete CSD platform.

However, even as we advocate for short-term deterrence measures to improve responsiveness to information-based threats, we must continue to engage in long-term knowledge and relationship building initiatives. Sustained investment in education and exchange programs remains the best antidote to disinformation effects. Moreover, it is important to remember that the current focus on malign influence threats is nothing new. Rather, it represents yet another in a series of technology-based efforts to protect USG national security interests in a complex information environment. We have always been—and always will be—at war over influence in the global information space.

ENDNOTES

[1] ACPD Data Call Request, “Public Diplomacy Program Data Call: Countering State-Sponsored Disinformation” (Jan 2017 - May 10, 2019).

[2] https://publications.armywarcollege.edu/pubs/3414.pdf.

[3] Joseph S. Nye, “Public Diplomacy and Soft Power,”*The Annals of the American Academy of Political and Social Science*, Vol. 616, March 2008, p. 99.

[4] https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf.

[5] https://www.bbc.com/news/world-us-canada-43719784.

[6] https://www.cnbc.com/2018/10/24/apples-tim-cook-warns-silicon-valley-it-would-be-destructive-to-block-strong-privacy-laws.html.

[7] P.W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (Boston: Houghton Mifflin Harcourt, 2018).

[8] https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf.

[9] Data drawn from a May 2019 ACPD survey of field-based CSD programs and initiatives.

[10] Hararo J. Ingram, *Persuade or Perish: Addressing Gaps in the U.S. Posture to Confront Propaganda and Disinformation Threats*, Program on Extremism, George Washington University,(February 2020), 11: https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Ingram%20Persuade%20or%20Perish.pdf.

[11] https://www.state.gov/state-defense-cooperation-on-global-engagement-center-programs-and-creation-of-the-information-access-fund-to-counter-state-sponsored-disinformation.

[12] See “About Us,” https://www.state.gov/about-us-global-engagement-center/ (Accessed June 2019).

[13] https://thehill.com/homenews/administration/387719-pompeo-lifts-hiring-freeze-at-state-department.

[14] See the ACPD’s *Comprehensive Annual Report on Public Diplomacy & International Broadcasting* for 2019 and 2020 (forthcoming), 131: https://www.state.gov/wp-content/uploads/2020/01/2019-ACPD-Annual-Report.pdf.

[15] https://www.foreign.senate.gov/imo/media/doc/082118_Mitchell_Testimony.pdf.

[16] https://www.state.gov/wp-content/uploads/2019/05/2018-ACPD.pdf.

[17] https://www.usagm.gov/2018/08/22/statement-from-ceo-john-f-lansing-on-agency-rebrand/.

[18] *Targeted Inspection of the Governance of the United States Agency for Global Media*, Office of the Inspector General, United States Department of State (April 2019), 10. https://www.stateoig.gov/system/files/isp-ib-19-22_0.pdf.

[19] *Embarking on Reform of the Office of Cuba Broadcasting*, U.S. Agency for Global Media (May 21, 2019): https://www.usagm.gov/wp-content/uploads/2019/05/Embarking-on-OCB-Reform-English.pdf.

[20] USAGM, “Expanding View of Current Time” (Internal Document, 2018).

[21] See Steven Erlanger, “What is RT?” *New York Times*, March 8, 2017: https://www.nytimes.com/2017/03/08/world/europe/what-is-rt.html.

[22] Yelena Osipova-Stocker and Nick Shchetko, *Addressing Disinformation: Insights and Best Practices, Office of Policy Research*, U.S. Agency for Global Media, 2020.

[23] https://www.washingtonpost.com/world/national-security/state-department-to-take-a-step-into-the-digital-age-in-effort-to-counter-disinformation/2019/04/12/c333bd8c-1b46-44d9-a2be-83aa0c8e9114_story.html.

[24] https://www.state.gov/acpd-official-meeting-minutes-september-4-2019/.

[25] While some bureaus indicated that they refer to counter-disinformation programming with other terminology, none of the research methods the ACPD pursued – including direct outreach – reflected the same amount of attention as in EUR. The challenges generated by using different terminology and strategic approaches have been noted elsewhere in this report.

[26] https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf.

[27] https://securingdemocracy.gmfus.org/advanced-persistent-manipulators-part-one-the-threat-to-the-social-media-industry/.

[28] Author interview with senior official, April 2019.

[29] Author interview with senior official, October 2018.

AUTHOR BIOGRAPHIES

Vivian S. Walker

Vivian S. Walker is the Executive Director of the United States Advisory Commission on Public Diplomacy. She has served as Faculty Fellow at the USC Center on Public Diplomacy (CPD), the Guest Editor for the CPD *Perspectives* series, an Adjunct Professor at the Central European University's (CEU) School of Public Policy and a Research Fellow at the CEU Center for Media, Data and Society. She has also been a Professor of National Security Strategy at the National War College in Washington, DC and the National Defense College of the United Arab Emirates.

In her 26-year career with the State Department, she rose to the senior executive rank of Minister Counselor. She twice served as a Deputy Chief of Mission (Croatia and Armenia), twice as an Office Director (Southeastern European Affairs and the Office of Press and Public Diplomacy for Europe), a Public Affairs Officer (Kazakhstan, with coverage of Tajikistan and Turkmenistan), a Cultural Affairs Officer (Tunisia) and an Information Officer (Haiti). Other assignments include a two-year professorship in strategic studies at the National War College, a yearlong assignment as the State Department's Regional Border Coordinator in Afghanistan, and a fellowship on the Atlantic Council, where she led the first interagency discussion on public diplomacy in the aftermath of the 9/11 terror attacks.

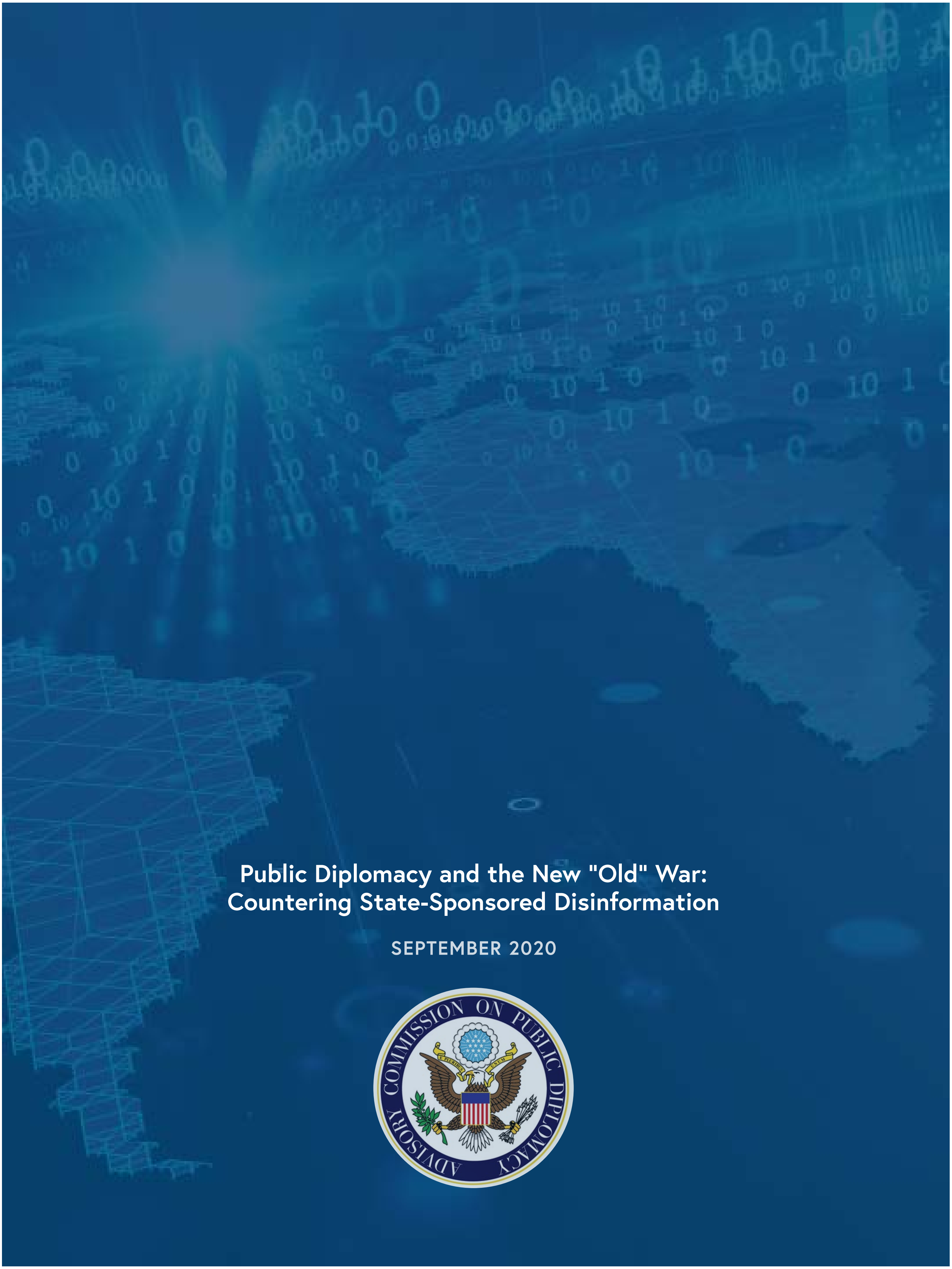
Dr. Walker has published and lectured extensively on the practice of public diplomacy in complex information environments. She graduated from Georgetown University's School of Foreign Service and earned her doctorate in English language and literature from the University of Chicago. She speaks French, Russian, and Croatian.

Ryan E. Walsh

Ryan E. Walsh serves the Department of State as Senior Advisor in the Bureau of Global Public Affairs (GPA). In this capacity, he identifies, designs, and implements digital and mobile innovations to public diplomacy programming in order to establish effective, ongoing engagement with foreign audiences. Prior to the merger that created GPA, he led Digital Product in the Bureau of International Information Programs. His previous work with ACPD includes authoring insights into a project which he directed, "U.S. 2016 Elections: A Case Study in 'Inoculating' Public Opinion Against Disinformation," in the report *Can Public Diplomacy Survive the Internet?* (2017).

Prior to government service, Mr. Walsh was on the launch team of a pioneering data-mining digital news startup that averaged over 5 million unique monthly visitors in its first year. For this work, which included publishing an investigative report that caused Facebook to change its terms of service as it relates to gun transactions on its platform, Mr. Walsh was recognized for *Digital Innovation in Journalism* by the Scripps Howard Foundation in 2014. Earlier, as a Crisis Management Analyst at Goldman Sachs, he responded to global incidents ranging from natural disasters, to terrorism, social unrest, and political instability. He began his career with the New York-based advertising agency Momentum Worldwide (McCann Worldgroup), advising Fortune 500 clients on disintermediation in the communications environment and the emerging power of digital communities.

Mr. Walsh holds a B.A. in History from Providence College in Rhode Island and a M.S. in Global Affairs from New York University. His thesis at NYU was titled *A Warning for the West: Connection Technologies and Social Unrest* (2012).



Public Diplomacy and the New "Old" War: Countering State-Sponsored Disinformation

SEPTEMBER 2020

ADVISORY COMMISSION ON PUBLIC DIPLOMACY